الفصل الأول

تعريف الشبكات الخاصة الافتراضية

1-1المقدمة :

في عصر اقل ما يقال عنه انه عصر التكنولوجيا وسرعة المعلومات .. عصر أصبحت فيه المعلومات هي العنصر الرئيس في جميع تحركاننا وتنقلاتنا وتحديد مرابحنـــــــــــــــــــا وحتـــــــــــــــــــى خســـــــــــــــــــائرنا

ومع ازدهار وتطور أساليب التقنية الحديثة وحتى تواكب الركب في توسع وانتشار الشركات العالمية كان لابد من إحداث ثورة في مجال الاتصالات الشبكية السلكية منها واللاسلكية بين فروع هذه الشركات ..

فعلى سبيل المثال يعتبر تواصل الفرع الرئيسي لشركة مايكروسوفت العملاقة مع احد فروعها في دولة ماليزيا والتناقش حول قضية وجود ثغرة أمنية اكتشفها خبراء مايكروسوفت في معامل روسيا أمرا بالغ السرية وبالغ الخطورة أيضا وبالمقابل فأن إجراء مكالمات هاتفية مطولة كهذه قد تسبب في إنهاك ميزانية اكبر الشركات إذا ما وضعنا في عين الاعتبار إجراء مكالمات على مدار الساعة وإتمام العمليات هاتفيا ..

لذا كان الحل موجودا وسهلا وممكنا للجميع وهنا تبدأ احد فوائد الانترنت الجمة في إتمام عمليات التواصل بين الأطراف المعنية بأقل التكاليف .

لكن الانترنت أفضل مافيه انه باب مفتوح للجميع وأسوأ مافيه انه أيضا باب مفتوح للجميع وهنا يبدأ القلق ...

أسئلة تطرح على مدار الساعة .. هل أنا مراقب ؟؟؟ هل اخترق أحد جهازي ؟؟ هل تمت سرقة هذه البيانات ؟؟؟ والكثير الكثير منها !!!

أسئلة قد لا تلج إلى عقول المستخدمين العاديين للانترنت .. فجل ما تحتويه أجهزتنا هي بعض من الملفات والتي حتى وان فقدت فمصدرها الرئيسي الانترنت و بالتالي

سنعيد تحميلها مرة أخرى .. أو أن نخسر اشتراكا تبقى منه لحظات قليلة لن يستمتع من سرقه بها ..

قد تكون خسارة البريد الالكتروني من أكبرها وقعا في النفوس لأنها شيء من الخصوصية والتي يكره الإنسان بطبيعة حاله أن يفقدها أو يعرضها على الغير .. كل هذه الخسائر لا تعني شيئا في الحقيقة إذا ما قارناها بخسارة بحث أمضى صاحبه الشهور الكثيرة وسهر الليالي الطويلة ليفقده في ليلة مظلمة ... لكن ماذا عن المستخدمين الحقيقيين للشبكة العنكبوتية ؟ ماذا عن أصحاب رؤوس الأموال والذين تتم معاملاتهم من بيع وشراء عن طريق هذه الشبكة ؟

من هذا المنطلق بدا ما يسمى ببرامج الحماية وبدأت كلمة الحماية تطفوا على السطح وتثبت أقدامها في مجال واسع وعالم مفتوح هو عالم الانترنت ... لكن السؤال الذي يطرح نفسه هنا : هل أنا بالفعل إذا قمت باتخاذ جميع سبل الحماية فأنني وبياناتي في أمان ؟

لن أجيب على هذا السؤال بأفضل ما أجاب خبير أمن الشبكات Peter Norton حيث قرأت له في إحدى كتبه انه قال (الجهاز الوحيد المؤمن والمحمي بنسبة 100% من أي مخاطر للسرقة والاختراق هو جهاز يوضع في زاوية الغرفة ولكنه لا يشبك نهائيا على الانترنت .....)

وكما قيل (الحاجة أم الاختراع) من هذا المنطلق بدأت الشركات الكبيرة وحتى الصغيرة النامية بالبحث عن سبل أخرى لحل هذه المشكلة وحتى لو بالالتفاف عليها ...

وكان لهم مبتغاهم ولو الى 95% حيث تم اكتشاف ما يسمى بـ

(Virtual Private Networking) VPN الشبكات الافتراضية الخاصة

1-2ماهي الـ VPN :

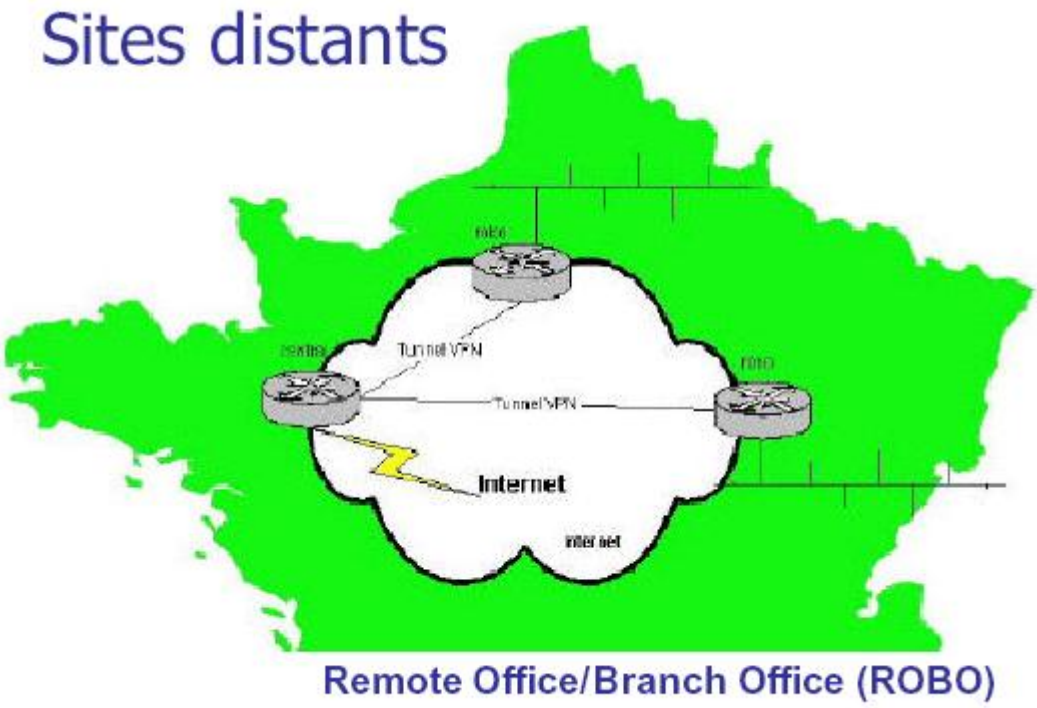
الاسم يدل على كونية هذه الشبكات فهي شبكات افتراضية لا وجود لها في الواقع ولكنها مع ذلك تؤدي واجبها على أكمل وجه كأكثر أنواع الشبكات أمانا وأكثرها شيوعا وحتى

استخداما بين الشركات الكبيرة ..

طبعا كونها شبكات افتراضية فلابد من وجود داعم حقيقي يحمل هذه الافتراضية الى ارض الواقع .. لابد لهذا الداعم أن يكون مستيقظا كل الوقت جاهزا ومستعدا في أي لحظة وهنا كانت الشبكة العنكبوتية لتثبت أنها دائما الأرض الخصبة لكل من أراد الثمر بقليل من الجهد

في الغرس والسقاية ...

هذه الشبكات الافتراضية هي نفسها الشبكة العنكبوتية لكن تم توظيف خصائصها لتلائم سرية نقل البيانات والحفاظ على امن المعلومات ..



1-3 كيف تعمل الشبكات الافتراضية ؟

حتى نستطيع فهم آلية عمل الشبكات الافتراضية لابد من التوقف قليلا عند آلية عمل الشبكة العنكبوتية أو غيرها من الشبكات في البداية .. لن أتعمق كثيرا في وصف آلية العمل لكن سأتطرق الى ما يهمنا منها .. قد لا يخفى على الكثير منكم بأن البيانات المرسلة عن طريق الانترنت ولنقل على سبيل المثال الرسالة التي يرسلها الشخص منا الى صديقه في الطرف الآخر من العالم عن طريق البريد الالكتروني تتحول الى طرود صغيرة تحتوي على معلومات مترابطة يتم تجميعها عند الطرف الآخر وهو المستقبل .. يتم تقسيم هذه الرسالة الى أقسام صغيرة بحيث تسهل عملية نقلها وتساعد في عملية إسراع النقل أيضا ...

لكن هذه الطرود أو الحزم المعلوماتية غير آمنة مطلقا وقابلة للخسارة إذا ماعرفنا أن الحزمة لابد وان تصل الى محطتها الأخيرة في 15 قفزة متتالية تتم بين أجهزة من الدرجة الثانية من مستويات الذكاء تسمى بالراوترز (Routers) حيث يقوم هذا الجهاز بتقسيم هذه العينات والتحكم بمسارها معتمدا بذلك على معلومات توفرها له الأجهزة المماثلة والقريبة منه بحيث تقفز كل حزمة اقل من أو 15 قفزة فقط حتى تصل الى محطتها الأخيرة وهي عند المستقبل وإلا فان هذه الحزمة تضيع ...

بالنسبة للشبكة العنكوبتية بشكل عام لا تحدث عمليات الخسارة المعلوماتية دائما ولكنها متوقعة إذا ما تعطل احد هذه الأجهزة ...

لكن ما لفرق بين الشبكة العنكبوتية العادية والشبكة الافتراضية ؟

هنا يبدأ مفهوم الأمن والحماية والحرص على الخصوصية في نقل المعلومات والبيانات

1-4 كيف تتم حماية البيانات في الشبكة الافتراضية ؟

تتم حماية البيانات بشكل عام عادة بتشفيرها بحيث يصعب فهمها إذا ما تمت سرقتها ... لكن أيضا حتى تشفير المعلومات لا يكفي أحيانا إذا وضعنا بعين

الاعتبار وجود أنواع كثيرة من آليات التشفير والتي يمكن كسرها بطريقة أو بأخرى وما أكثر الأمثلة هنا ابتداءها بسرقة أرقام البطاقات الائتمانية وانتهاءاً بسرقة البرامج القيد البرمجة من أصحابها وغيرها الكثير من الأمثلة ... لذلك كان لابد دائما من إتباع خوارزميات قوية ومؤكدة من شركات كبيرة وذات اسم لامع في عالم التشفير كنقطة مبدئية للعمل على هذه الشبكات الافتراضية ...

هنا تظهر مشكلة أخرى وهي أن المعلومات التي يتم إرسالها بين الشبكتين كما عرفنا مسبقا يتم تقسيمها الى حزم صغيرة يتم إرسالها باستخدام بروتوكولات متعددة تعتمد على طبيعة الشبكة والمعلومة مما قد يسبب ضياع هذه المعلومات وعدم الاستفادة منها إذا وضعنا في عين الاعتبار عجز الشبكة المستقبلة لهذه الحزم على فهمها نتيجة لعدم تعرفها على طبيعتها لذا كان من الواجب إيجاد حل وسطي وسلمي وآمن في نفس الوقت وهذه ما قدمته شركة

(Tunneling) حيث اقترحت هذه الشركة أن يقوم بإرسال الحزم المعلوماتية في طرود عادية في داخل طرود أخرى تكون مشفرة بحيث أن الطرود الحاوية على الطرود المعلوماتية تكون مفهومة لدى الشبكة المستقبلة .. وبهذا تحل مشكلة قراءة هذه الحزم المعلوماتية ..

1-5 مكونات الشبكة الافتراضية :

بشكل عام تتكون الشبكات الافتراضية من مكونين أساسيين أولهما العميل (Client) وثانيهما بوابة الاتصال (Gateway) ..

- **وظائف بوابة الاتصال (Gateway) :**

تنقسم بوابة العبور الى قسمين (Software& Hardware) موجودة في مقر الشركة .

في معظم الشركات تتوفر الشبكات المحلية والتي تربط أجهزة الشركة الواحدة ببعضها البعض (LAN) ولكل شبكة محلية شبكة افتراضية خاصة بها تعتبر

نقطة البداية والنهاية لهذه الشبكة تتحكم بها بوابة الاتصال والتي بإمكانها الاتصال بأكثر من عميل (Client) في الوقت الواحد باستخدام قنوات متعددة والتي تعتمد في عددها على مكونات الكمبيوتر الصلبة (Hardware) وسرعة الاتصال ..

تقوم بوابة الاتصال بالقيام بالعديد من المهام كبدأ وإعطاء الصلاحيات وإدارة القنوات بعد بدأ الاتصال بعد ذلك تقوم بوابة الاتصال بإيصال المعلومات الى الجهة الصحيحة على الشبكة .. كما أن بوابة الاتصال تقوم بعملية مهمة لغاية وهي عملية تشفير البيانات (Encryption) قبل إرسالها وتقوم بفك تشفيرها (Decryption)

عند استلامها ..

- **وظائف العميل (Client) :**

يقوم الجهاز العميل (Client) تقريبا بنفس مهام بوابة الاتصال إضافة الى ذلك انه يقوم بإعطاء تصاريح الدخول الى الشبكة على مستوى الأفراد المستخدمين ..

لابد من توفر بعض النقاط الضرورية إذا ما أخذنا بعين الاعتبار أن العميل هو حلقة الوصل بين طرفين فمن هذا المنطق وجب اخذ الحذر من احتمالات إصابة بعض الملفات المرسلة بفيروسات أو حتى حملها لملفات تجسس مما قد يخل بأمان الشبكة لذا كان من الضروري التأكد من وجود مكافح فيروسات قوي ومحدث بآخر التحديثات من الشركة الأم وأيضا لا يمكن الاستغناء عن جدار ناري للتأكد بأنه بالفعل حتى (لو) وجدت ثغرة بسيطة في هذه الشبكة فان هناك من يرصدها ويحميها ...

تحدثنا بما فيه الكفاية عن بوابة الاتصال وأيضا العملاء لنلقي الضوء على

الشبكة **الهدف أو (Target Network) :**

تعطي هذه الشبكة صلاحيات مرور محددة (Limited Access) لعبور الشبكة والوصول إلى البيانات أو المعلومات فكما يعرف الجميع انه بعد انتقال هذه البيانات من بوابة الاتصال فان البيانات تكون في فضاء الانترنت سهلة المنال لكل من أراد .. إن لم يكن هناك من يضبط حركة الوصول الى هذه البيانات وهنا تبدأ أهمية هذه الشبكة ..

كما أنها تعطي أيضا صلاحيات محددة لمن أراد الدخول الى الشبكة عن بعد (Remote Access) وذلك بضبط شروط معينة واعطاء صلاحيات والسماح لأشخاص معينين بالوصول الى معلومات معينة ... وتحديد مثل هذه الصلاحيات الى الوصول الى معلومات معينة أمر غاية في الأهمية إذا أخذنا بعين الاعتبار إمكانية وصول أطراف غير معنية الى هذه المعلومات فبترشيد البيانات والصلاحيات المعطاة الى الشبكات أو الاتصال البعيد تقل الخسائر الممكنة والمتوقعة إذا ما حصل واستطاع احد الوصول الى هذه الشبكة بطريقة غير
شرعية ...

أحب هنا أن أوضح نقطة مهمة وغاية في الأهمية فيما يتعلق بالحزم المعلوماتية بعد خروجها من بوابة الاتصال فهذه البيانات غير قابلة للتشفير (Unencrypted) بعد خروجها من بوابة الاتصال لذا فإن نظام حماية عالية الكفاءة أمر ضروري لا غنى عنه ...

1-6 من يستخدم نظام الشبكات الافتراضية ؟

تقوم هذه الشبكات على أي شبكة داخلية (LAN)وتستطيع أي شركة استخدام مثل هذه الشبكات الافتراضية للاتصال ببعضها البعض أينما كانت فروعها وذلك لأنها رخيصة التكاليف إن لم تكن معدومة أيضا ويلزمك لاستخدام مثل هذه الشبكة وجود نظام تشغيل داعم للشبكات مثل نظام التشغيل (Windows Server 2000) أو أي نظام مشابه

تتم عملية تنصيبه على جهاز يعتبر السيرفر تساعد أيضا هذه الشبكات رؤساء الشركات على الدخول الى الشبكة الداخلية

(Intranet) والخاصة بالشركة ومن ثم القيام بأعمالهم وهم في منازلهم كما ولو أنهم في مكاتبهم .. كما أنها تساعد الموظفين التنفيذيين على الاتصال بالشبكة من أي مكان في العالم فكل ما عليه فعله هو فقط شبك جهازه النقال بأي شبكة انترنت ومن ثم العبور عبر بوابة الاتصال بعد إثبات الهوية والدخول الى المعلومات التي يريدها كما لو انه في الشركة نفسها .

7-1 حماية البيانات:

يجب أن توفر VPN الخواص التالية لتأمين أمن المعلومات:

1- authentication - :الاستيقان : وتعني التأكد من هوية الشخص الذي يطلب المعلومات .

2- access control التحكم بالوصول للشبكة : وتعني التحكم بمن يستطيع الوصول للشبكة ، أي منع الأشخاص الذين لا يملكون صلاحيات معينة من دخول الشبكة.

3- confidentiality السرية : منع أي كان من قراءة أو نسخ المعلومات التي تنتقل عبر
الشبكة.

4-data integrity سلامة المعلومات : منع أي تعديل للمعلومات عندما تعبر الشبكة.

ولقد استخدمت أنظمة كثيرة من أجل الـ authentication من بينها كلمات السر، وهنا ظهر العديد من البروتوكولات من أجل الاستيقان مثل PAP (password authentication protocol) أي بروتوكول الاستيقان بواسطة كلمة السر: ويتم خلاله تشفير كلمة السر وإرسالها عبر الشبكة ثم مقارنتها مع كلمة سر مخزنة على المخدم.

من البروتوكولات الأخرى

CHAP (Challenge Hand check authentication Protocol) الذي يتم فيه إرسال رقم عشوائي من المخدم للمستخدم نشفر بواسطته كلمة السر (تشفير غير عكسي) ثم نرسلها للمخدم الذي يقارنها مع كلمة السر الموجودة لديه.

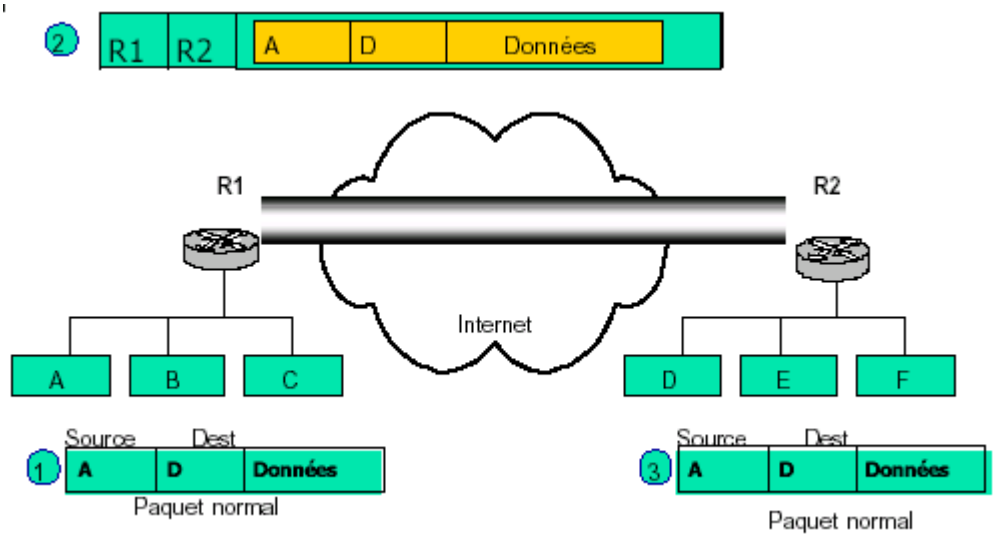
ولضمان مستوى أمن أعلى يمكن استخدام البطاقات والمفاتيح الذكية.

أما عن سرية وسلامة المعلومات أثناء عبورها الشبكة العامة فيتم استخدام التشفير ذو المفاتيح المتناظرة والغير متناظرة ، ولضمان مستوى عالي من السرية يجب استخدام مفاتيح تشفير طويلة ومن أشهر خوارزميات التشفير rijndael التي تعتبر المعيار العالمي في التشفير حالياً بالنسبة للخوارزميات متناظرة المفاتيح . ومن خوارزميات التشفير الغير متناظرة المفاتيح خوارزمية RSA .

8-1 تقنية الأنفاق:

encapsulation التغليف وهو عملية إنشاء بروتوكول افتراضي وحيد يصل بين أطراف الـ VPN مبني على البروتوكولات المتوفرة في الأجزاء التي نريد وصلها ببعض .

بمعنى آخر هو عملية تحويل البروتوكولات المستخدمة في أجزاء الشبكة (التي نريد ربطها مع بعض) لتصبح متوافقة مع بروتوكولات شبكة الإنترنت التي ستصل بين هذه الأقسام.



وهنا لدينا حالتين:

1: LAN-to-LAN tunneling وهي حالة ربط شبكتي LAN بواسطة VPN وفي هذه الحالة قد لا تكون الشبكتين تستخدمان نفس البروتوكولات وبالتالي تكون مهمة الـ tunneling هي تحويل البروتوكولات إلى بروتوكول IP ليصبح متوافق مع الإنترنت التي سينتقل عليها

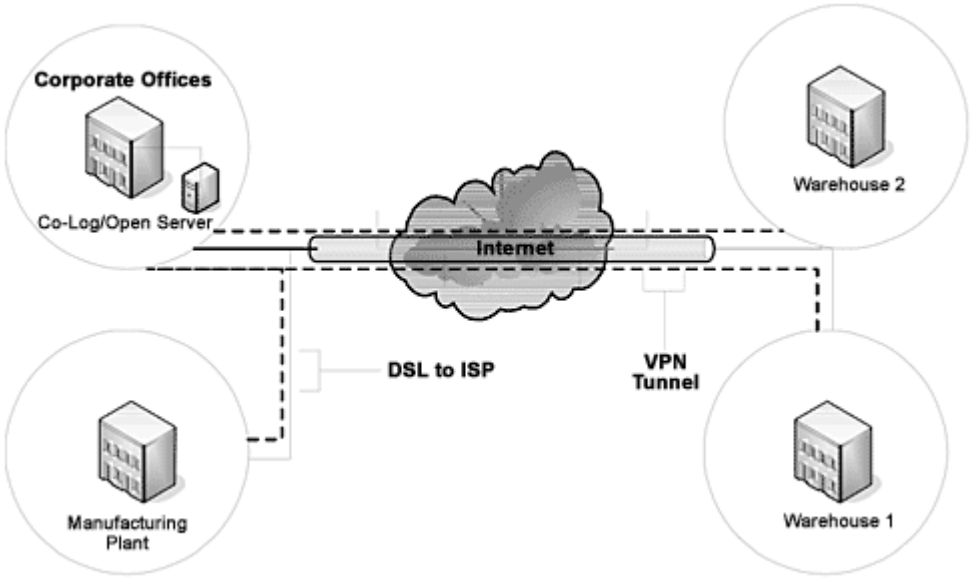
.

2: client-to-LAN tunnels

وهي حالة ربط حاسب وحيد بالشبكة الرئيسية للشركة. وهذه الحالة للموظفين المتنقلين الذين يتصلون بالشركة من منازلهم أو من أماكن أخرى أثناء سفرهم مثل الفنادق والمطاعم.

ومن بروتوكولات الـ tunneling :

point-to-point tunneling protocol (PPTP), layer-2 forwarding (L2F), layer-2 tunneling protocol (L2TP), and IP security prot



الفصل الثاني

استخدامات الشبكة الخاصة الافتراضية

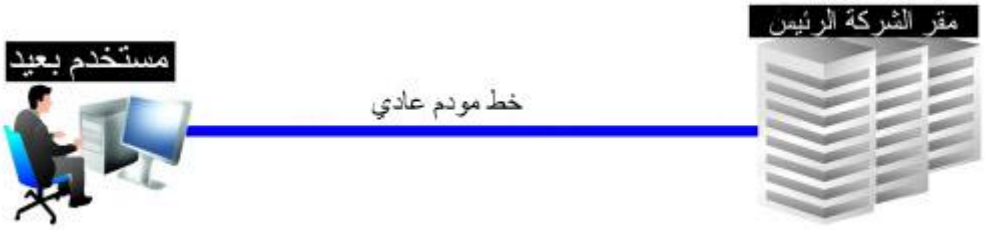
2-1 مقدمة:

تتردد كثيرا من الشركات في استخدام الشبكات الافتراضية الخاصة لأنها متخوفة من أعطال الإنترنت وضعف الأداء. وهو خوف لا ينبغي أبدا أن يكون السمة الغالبة على مواقف الشركات وعقليتها في التفكير. وهذا يجعلنا نستعرض بعض الأمثلة العملية لبعض الشركات التي اتخذت قرارا بتنفيذ الشبكة الافتراضية لديها لما تقدمه هذه التقنية من خدمات عظيمة نستعرضها خلال هذا الفصل:

2-3 خدمة النفاذ عن بعد (Remote Access Service):

إن فكرة الشبكات الافتراضية الخاصة قد ساهمت في تخفيض تكاليف نقل المعلومات الخاصة بالشركات و المؤسسات بين فروعها البعيدة عن المقر الرئيسي لها و بين المستخدم المنزلي الذي يريد الوصول إلى معلوماته المتوفرة في جهاز الحاسب المنزلي.قد تملك شركة من الشركات مكتباً واحداً, و قد تملك مكاتب كثيرة موزعة في أنحاء مختلفة من البلاد أو خارج البلاد. قد يعمل موظفوها من المكتب الرئيس لها أو من خلال المكاتب الموزعة في أنحاء البلاد أو حتى من خلال بيوتهم أو مواقعهم البعيدة كحقول النفط في البحار. في الماضي, كان المستخدم البعيد أو الموظف الذي يعمل من منطقة بعيدة عن المقر الرئيس للشركة يتصل من خلال مودم عادي للشركة باستخدام خطوط الهاتف. يقوم سرفر و مودم أخر موجودان في مقر الشركة بالرد على اتصال الموظف ليقوم بعمله و يتم إقفال الخط بعد الانتهاء من العملية. سلبيات هذه الطريقة كانت من عدة نواحي منها كلفة فواتير الهاتف للمستخدم البعيد, إيجار الخطوط ,سرعة الاتصال البطيئة ,بالإضافة الى إشغال خط الهاتف أثناء فترة الاتصال. رغم هذه السلبيات كانت العملية نوعاً ما آمنة لأنها كانت تصل الطرفان بشبكة مغلقة و مسار خاص. كانت الشركات المقتدرة تستخدم

خطوط عالية السرعة تسمى بالـ Leased Lines لتتغلب على مشكلة السرعة لكنها كانت تدفع مبالغ ضخمة في مقابل هذه الخدمة لربط النقطتين بشكل متواصل و بسرعة عالية و بشبكة خاصة آمنة نوعاً ما.



عندما انتشرت شبكة الانترنت في كل مكان, كانت هناك فرصة استخدامها كوسيط لنقل المعلومات و كشبكة يمكن من خلالها نقل المعلومات من مكان الى آخر بأسعار زهيدة مقارنة بالطريقة السابقة, و لم يكن هناك داعٍ لتوصيل نقطتين مع بعضها فيمكن الاتصال من أي جهاز في العالم بأي جهاز في العالم إن كانا متصلين بالانترنت. و إن كانت نوعية الاتصال بين الجهازين هو الـ ADSL فان التكلفة تكون ثابتة و مناسبة و الاتصال قائم بشكل مستمر.

أما في الشبكات الافتراضية الخاصة فقد تم استبدال الطلب الهاتفي التقليدي بالشبكة الافتراضية مما خفض كلفة الاتصال بشكل كبير جداً حيث تم تخفيض الكلفة على

النصف و رفع الأداء إلى الضعف مقارنة مع الاتصالات العادية

(و بشكل خاص الاتصالات الدولية).

4-2 توسيع الشبكات المحلية:

إن توسيع الشبكات المحلية يتطلب اتصالا مستمراً على مدار الساعة والذي يعني تكاليف اتصال مرعبة خاصة في الاتصالات الدولية,تقدم VPN وسيلة لربط هذه الشبكات و بكلفة معقولة جداً عبر نمطين للاتصال:

4-2-1-VBN Extranets:

تبدي الكثير من المؤسسات في القطاعات التجارية و الصناعية، والمؤسسات الحكومية استعداداً متزايداً لتبني إحداث هذه الحلول التقنية.حيث أن الاتصالات فائقة السرعة أصبحت تشكل مطلباً أساسياً للصناعات الكبرى كنتيجة للاقتصاد العالمي المتغير على مدار الساعة فلا يوجد ما يمنع هذه المؤسسات من الاستفادة من الشبكات التي استثمرت مبالغ كبيرة في بنائها حتى تصل إلى هذا المستوى الذي يؤهلها لتكون وسيلة الربط الآمنة و الجاهزة في كل لحظة لتزيد من قدرة هذه المؤسسات على توفير المعلومات اللازمة دعما لاتخاذ القرار و نقل تغيرات السوق بشكل آني ,كما أنها تشكل و وسيلة أساسية و لاغنى عنها لربط

الموزعين بشركتهم الأم.

و بالتالي أصبحت هذه الشبكات تساهم كثيراً في تطوير سير العمل في شتى قطاعات الأعمال لدرجة أن كثير من الشركات قد باتت تعتمد عليها اعتماداً كلياً، ومعظمها يسند إلى هذه الشبكات مهام تشغيل نظام إدارة موارد الشركة ونظام الحسابات بعد أن تأكدت من وصول أداء شبكاتها إلى مستوى يمكن الاعتماد عليه، وأظن أن هذه التطبيقات أصبحت أكثر أهمية لدى هذه الشركات من إجراء المكالمات الهاتفية. ويجمع الكثيرون على استعداد البنية التحتية والشبكات لاستيعاب هذا الاستخدام الجديد لها، فما عدنا نسمع تساؤلات تشكك في قدرة هذه الأخيرة على إتمام هذه المهام بالمستوى المطلوب، وقد أصبح ذلك راسخاً في فكر مدراء تقنيات المعلومات وأصحاب القرار في هذه الشركات الكبرى".

من خلال هذا الدعم الكبير الذي تقدمه الـ VBN فقد أصبحت خياراً استراتيجياً للعديد من الشركات

2-4-2 VPN Intranets:

إن مصطلح Intranets يستخدم عادة للإشارة إلى شبكات الشركات أو الجامعات أي تجمع لعدة شبكات محلية بمعنى آخر إن Intranets هي أحد أشكال الـ WAN .

لتحقيق انترانت لشركة ما فإن الأساليب المستخدمة متنوعة بدلاً من كابلات Ethernet على المسافات القريبة و صولاً للكابلات الضوئية و الشبكة الهاتفية على المسافات البعيدة .

إن ربط هذه الشبكات عبر القارات هاتفياً هو عملية مكلفة جداً و من النادر أن تكون ذات مردود مقبول من حيث نوعية الاتصال ,و هنا يأتي دور الـ VPN حيث قامت بحل هذه المشكلة عن طريق استثمار الشبكة العنكبوتية العالمية المتواجدة أساساً لتؤمن الوصل بين القطاعات الجغرافية المتباعدة و العائدة لنفس الشركة.

الفصل الثالث

VPNالميزات والمساوئ

جذبت الشبكات الخاصة الافتراضية VPN اهتمام العديد من المؤسسات لتوسيع شبكتها بكلفة قليلة. ويمكن أن نجدها حالياً في بعض المنازل وأماكن العمل(فنادق – مطاعم) حيث يُسمح للموظفين بدخول شبكة الشركة بطريقة آمنة. وأصبحت VPN تستخدم للبقاء متصلين بشبكة الشركة بشكل دائم، كما أنها تؤمن ربط فروع الشركة ببعضها أيضاً.

سواء كنت مهتم بالـ VPN أم لا ، فدراستها مشوقة لأنها تحوي العديد من المفاهيم الهامة مثل بروتوكولات الإنترنت ، أمن الإنترنت وغيرها.

الشبكة الخاصة الافتراضية هي شبكة تستخدم شبكة عامة لنقل المعلومات بطريقة آمنة عوضاً عن استئجار خطوط خاصة . Leased Lines ومن أكثر أنواعها انتشاراً Internet VPN : أي التي تستخدم الإنترنت كشبكة عامة لنقل المعلومـــــــــــــات .

فمثلاً بإمكانك إنشاء VPN بين حاسبك بالمنزل وبين حواسب الشركة التي تعمل فيها مستخدما بذلك الإنترنت لنقل المعلومات ومستخدماً التشفير لضمان سلامة وسرية معلومات الشركة .

وطبعاً يتم تطبيق الـ VPN على شبكات .WAN لتصبح أفضل من PrivateWANبتوفرها الدائم و أداءها الأفضل، كما أنها أقل كلفة وأكثرأمناً وفعالية.

فتخيل أنك تريد إنشاء شبكة بين فرعين من شركة واحدة في بلدين مختلفين، فإذا فكرت باستئجار خط هاتفي فإنه سيكلف كثيراً كما أنه خط وحيد مما يشكل خطر على الاتصال في حال ظهور مشكلة في خط الاتصال ، بالإضافة إلى أن المعلومات عليه قد لا تنتقل بشكل آمن. لذلك الحل الأمثل هو استخدام شبكة

الإنترنت ذات الكلفة القليلة والتي تؤمن اتصال بشكل دائم ، كما يجب تشفير المعلومات لضمان سلامة المعلومات.

من ميزات VPN أنها تسمح لك الاتصال بمزود خدمة الإنترنت ISP بأي وسيلة ترغب بها (مودم (... DSL – ISDN – بدون أن نكون بحاجة لإضافة أي تجهيزات إضافية في المقر الرئيسي للشركة، فالمقر الرئيسي بحاجة لمخدم VPN يصلنا بشبكة الإنترنت بدلاً من التجهيزات المعقدة التي تستخدم في الطرق التقليدية (مجموعة من الموديمات ، مجموعة من دارات ربط (... WAN كما أن استخدام VPNيقلل من الدعم الفني اللازم لأن مزود خدمة الإنترنت ISP هو الذي يقوم بالدعم الفني للشبكة .

بمعنى آخر : في حالة عدم استخدام VPN علينا القيام بمهام ISP كاملة بالإضافة لعمليات أمن أخرى ، أما في حال استخدام VPN فإننا نستفيد من الخدمات التي يقدمها ISP وبالتالي نخفف من العمليات والدعم الواجب تنفيذه.

3-1 خواص VPN لتأمين أمن المعلومات:

يجب أن توفر VPN الخواص التالية لتأمين أمن المعلومات :

1- **الاستيقان authentication**: وتعني التأكد من هوية الشخص الذي يطلب المعلومات

2-**التحكم بالوصول للشبكةaccess control** : وتعني التحكم بمن يستطيع الوصول للشبكة ، أي منع الأشخاص الذين لا يملكون صلاحيات معينة من دخول الشبكة.

3-**السريةconfidentiality** : منع أي كان من قراءة أو نسخ المعلومات التي تنتقل

عبر الشبكة.

4- **سلامة المعلوماتdata integrity** : منع أي تعديل للمعلومات عندما تعبر الشبكة.

ولقد استخدمت أنظمة كثيرة من أجل الـ authentication من بينها كلمات

السر، وهنا ظهر العديد من البروتوكولات من أجل الاستيقان مثل PAP :
(password authentication protocol)أي بروتوكول الاستيقان بواسطة كلمة السر: ويتم خلاله تشفير كلمة السر وإرسالها عبر الشبكة ثم مقارنتها مع كلمة سر مخزنة على المخدم من البروتوكولات الأخرى CHAP (Challenge Hand check authentication Protocol)الذي يتم فيه إرسال رقم عشوائي من المخدم للمستخدم نشفر بواسطته كلمة السر (تشفير غير عكسي) ثم نرسلها للمخدم الذي يقارنها مع كلمة السر الموجودة لديه.

ولضمان مستوى أمن أعلى يمكن استخدام البطاقات والمفاتيح الذكية.

أما عن سرية وسلامة المعلومات أثناء عبورها الشبكة العامة فيتم استخدام التشفير ذو المفاتيح المتناظرة والغير متناظرة ، ولضمان مستوى عالي من السرية يجب استخدام مفاتيح تشفير طويله.

العنصر الثاني الذي يجب التحدث عنه عندما نتكلم عن ال VPN هو tunneling و encapsulation التغليف) وهو عملية إنشاء بروتوكول افتراضي وحيد يصل بين أطراف ال VPN مبني على البروتوكولات المتوفرة في الأجزاء التي نريد وصلها ببعض .

بمعنى آخر هو عملية تحويل البروتوكولات المستخدمة في أجزاء الشبكة (التي نريد ربطها مع بعض) لتصبح متوافقة مع بروتوكولات شبكة الإنترنت التي ستصل بين هذه الأقسام.

وهنا لدينا حالتين:

1- **LAN-to-LAN tunneling** حالة ربط شبكتي LAN بواسطة VPN

وفي هذه الحالة قد لا تكون الشبكتين تستخدمان نفس البروتوكولات وبالتالي تكون مهمة ال tunneling هي تحويل البروتوكولات إلى بروتوكول IP ليصبح متوافق مع الإنترنت التي سينتقل عليها.

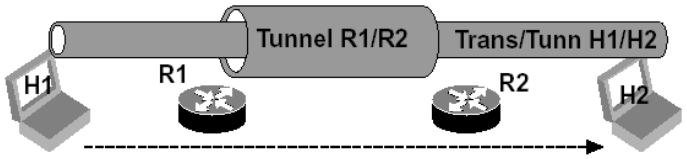


Exhibit 7-7. Gateway-to-gateway VPN using tunnel mode with transport or tunnel mode between internal hosts.

2-**client-to-LAN tunnels** حالة ربط حاسب وحيد بالشبكة الرئيسية للشركة. وهذه الحالة للموظفين المتنقلين الذين يتصلون بالشركة من منازلهم أو من أماكن أخرى أثناء سفرهم مثل الفنادق والمطاعم.

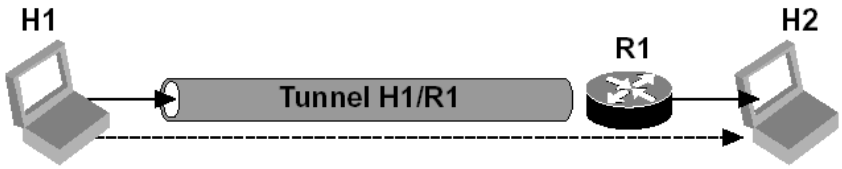


Exhibit 7-5. Host-to-gateway VPN using tunnel mode: a typical remote access solution.

ومن بروتوكولات ال tunneling : point-to-point tunneling protocol (PPTP), layer-2 forwarding (L2F), layer-2 tunneling protocol (L2TP), and IP security protocol (IPSec).

يتوفر في السوق نوعين من الـ VPN : برمجي Software أو . Hardware وبإمكاننا إنشاء VPN برمجية باستخدام شبكة Win2000 Server من Win2000 Clients أو WinXP clients حيث تم دمجها مع نظام التشغيل ليتم تطبيقها بطريقة سهلة من خلال استخدام Active Directory الموجود في Win2000 Server حيث يمكن استخدام بروتوكول IPSec الذي يساهم في أمرين أساسيين : تشفير المعلومات و عملية Tunneling وبعد إنهاء تصميم VPN في Windows بإمكاننا اختيار أن يكون الاستيقان authentication من خلال كلمة سر أو من خلال بطاقة ذكية.

وأخيراً نذكر مساوئ الـ VPN : إنها تتطلب معرفة عميقة بمواضيع أمن الشبكة، كما أنها متعلقة بعوامل خارجية لا يمكن التحكم بها كونها تعتمد على الإنترنت ، بالإضافة لعدم توافقية منتجات الـ VPN من الشركات المختلفة.

وبالتالي ومن خلال ماسبق يمكن اتخاذ القرار الانسب باستخدام VPN اوعدم استخدامها اخذين بعين الاعتبار عامل الكلفة والسرعه والأداء والوثوقية والامن وعلى اساسها نختار القرار الأنسب

الفصل الرابع

التشفير

من المستحيلُ مُنَاقَشَة IPsec VPNs بدون فَهْم المبادئ الأساسيه للتشفير. تُعرّفُ معاييرُ IPsecعِدّة أنواع التشفيرِ حالياً التيـيُمْكِنُ أَنْ تستَعملَ (DES, 3DES, RC5, IDEA, CAST, BlowFish, 3IDEA, and RC4) لحِماية المعلومات. حملت لنا الإنترنت التي تضم مجموعة كبيرة من الشبكات حول العالم فوائد جمة، وأصبحت وسيلة سهلة وممتعة تُتيح لملايين البشر الولوجَ إلى كم هائل من المعلومات، إضافةً إلى التواصُل وتبادُل المعلومات والرسائل فيما بينهم. ولكن بعض العوامل (مثل الطبيعة المفتوحة لهذه الشبكة، وعدم وجود أي جهة يمكنها الادعاء بأنها تمتلكها أو تسيطر عليها، وعدم وجود قوانين مركزية رادعة)– أدَّت إلى انتشار العديد من الجرائم السيبيرية (أي جرائم على الشبكة) مثل: التجسس على حُزَم الرسائل (packet sniffing)، وكذلك تخريب أجهزة الكمبيوتر وملفاتها (computer hacking)، وَشَنّ هجوم الفيروسات على البريد الإلكتروني، إضافة إلى عمليات الخداع (hoaxes) وغيرها. ورغم أن الإنترنت ليست البيئة الوحيدة التي تحدُث فيها الجرائم والمخالفات القانونية، إذ إن الجريمة ظاهرة موجودة في مجتمعات عديدة، فإن المشكلة الرئيسة تكمن في عدم وجود قوانين دائمة ورادعة تحمي مستخدمي الإنترنت. ومما سبق نجد أن أمن الإنترنت أصبح شأناً مهماً لا بد من حل مشاكله، نظرا لأهمية هذا الأمن في عمليات تبادُل المعلومات الشخصية ومعلومات العمل.وتشكل قضايا الأمن والتهديدات الناتجة عنها العائق الأكبر أمام اكتساب ثقة الناس ومشاركتهم في تقدم الإنترنت، وإجراء الحركات المالية عبرها. وتبقى مسألة الحفاظ على أمن الإنترنت باعتماد وسائل سهلة واقتصادية من أكثر المسائل التي تشكِّل حالياً تحدياً كبيراً لهذه التقنية.

4-1 تحديات الأمن:

يتلخص هدف جميع مستخدمي الإنترنت في الحصول على المعلومات ونقلها بشكل آمن، وهناك مجموعة من التحديات التي يجب أخذها في الحسبان لضمان نقلٍ آمن للمعلومات بين الأطراف المتصلة، وتنحصر هذه التحديات في ثلاثة محاور هي: الخصوصية (privacy)، وسلامة المعلومات (Integrity)، والتحقق من هوية الأطراف الأخرى (peer authentication).

4-2 خصوصية المعلومات (Privacy):

كي تتم المحافظة على خصوصية الرسالة الإلكترونية، يجب ألا يتمكَّن من الاطلاع عليها إلا الأطراف المعنية المسموح لها بذلك. وللحفاظ على الخصوصية، لا بُدَّ من التحكم بعملية الولوج، وأكثر طرق التحكم انتشاراً هي: استخدام كلمات المرور (passwords)، والجدار الناري (firewall)، إضافة إلى شهادات الترخيص (authorization certificates). وهنا، تجدُر الإشارة إلى أمر بالغ الأهمية؛ وهو أن على المستخدِم الحفاظ على سرية كلمة المرور، لأنها تشكل خط الدفاع الأول في وجه الولوج غير المُرخَّص. وبهذه الطرق، يُمكن منع حدوث الجرائم المتعلقة بانتهاك الخصوصية مثل: التنصُّت (eavesdropping)، واستعراض معلومات معيَّنة بدون ترخيص.

4-3 سلامة المعلومات (Integrity) :

لا بُدَّ من حماية عمليتي نقل المعلومات وتخزينها، وذلك لمنع أي تغيير للمحتوى بشكل متعمَّد أو غير مُتعمَّد. وتكمن أهمية ذلك في الحفاظ على محتوى مفيد وموثوق به. وفي الغالب، تكون الأخطاء البشرية وعمليات العبث المقصود هي السبب في تلف أو تشويه البيانات. وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام.ولتلافي تشويه أو تلف البيانات، يُمكن استخدام تقنيات مثل: البصمة الإلكترونية للرسالة (message digest) والتشفير (encryption)، ومن المفيد أيضاً استخدام برمجيات مضادة للفيروسات (anti-software virus) لحماية أجهزة التخزين من انتهاكات الفيروسات التي تتسبب

في تلف أو تشويه البيانات. ومن المهم أيضاً الاحتفاظ بِنُسَخ احتياطية (backup) لاسترداد البيانات المفقودة في حال تعرضها للضرر، أو في حال تعطُّل الشبكة أثناء عملية النقل.

التحقق من هوية الأطراف الأخرى (Peer Authentication) يجب التأكد من هوية الأطراف المعنية بعملية تبادل البيانات، إذ يجب على كلا الطرفين معرفة هوية الآخر لتجنب أي شكل من أشكال الخداع (مثل عمليات التزوير وانتحال الشخصيات). وهناك بعض الحلول والإجراءات للتحقق من هوية الأطراف المتصلة مثل: كلمات المرور (passwords)، والتواقيع الرقمية (digital signatures)، والشهادات الرقمية (digital certificates) التي يُصدرها طرف ثالث. ويُمكن أيضا تعزيز الأمن بالاعتماد على بعض المميزات المحسوسة مثل: بصمة الإصبع (finger print)، والصوت، إضافة إلى الصورة.

4-4 التشفير

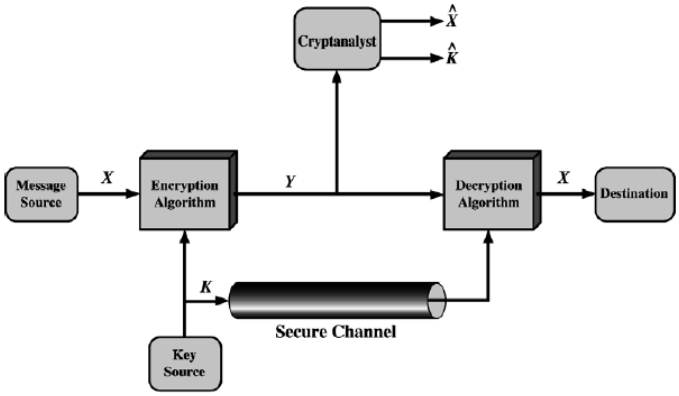
استخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب؛ خوفاً من وقوع الرسائل الحساسة في أيدي العدو. وقام يوليوس قيصر بتطوير خوارزميته المعيارية المعروفة باسم شيفرة قيصر (Caesar Cipher) التي كانت نصّا مشفَّراً (Cipher text)؛ لتأمين اتصالاته ومراسلاته مع قادة جيوشه. وظهرت فيما بعد العديد من الآلات التي تقوم بعمليات التشفير، ومنهاآلة التلغيز (Enigma machine).وشكَّل الكمبيوتر في بدايات ظهوره وسيلةً جديدة للاتصالات الآمنة، وفك تشفير رسائل العدو. واحتكرت الحكومات في فترة الستينيات حق التشفير وفك التشفير. وفي أواخر الستينيات، أسَّست شركة آي بي إم (IBM) مجموعةً تختص بأبحاث التشفير، ونجحت هذه المجموعة في تطوير نظام تشفير أطلقت عليه اسم لوسيفَر (Lucifer). وكان هذا النظام مثاراً للجَدَل، ورغم تحفّظات الحكومة الأمريكية علية لاعتقادها بعدم حاجة الشركات والمؤسسات الخاصة إلى أنظمة التشفير، إلا إنه قد حقق انتشاراً واسعاً في

الأسواق. ومنذ ذلك الحين، أخذت العديدُ من الشركات تقوم بتطويرَ أنظمة تشفير جديدة، مما أبرز الحاجة إلى وجود معيار لعمليات التشفير. ومن أبرز المؤسسات التي أسهمت في هذا المجال، المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standards and Technology- NIST) المعروف سابقاً باسم المكتب الوطني الأمريكي للمعايير (U.S. National Bureau of Standards)، إذ طوَّر هذا المعهد عام 1973 معياراً أطلق عليه معيار تشفير البيانات (Data Encryption Standard- DES). ويستنِد هذا المعيار إلى خوارزمية لوسيفَر (Lucifer algorithm) التي تستخدِم مفتاح تشفير بطول 56 بت (bit)، وتشترط أن يكون لكل من المرسِل والمستقبِل المفتاحَ السري ذاته. وقد استخدمت الحكومة هذا المعيار الرسمي عام 1976، واعتمدته البنوك لتشغيل آلات الصراف الآلي (ATM). وبعد عام واحد من تطبيق معيار تشفير البيانات (DES)، طَوَّر ثلاثة أساتذة جامعيون نظامَ تشفير آخر أطلقوا عليه اسم (RSA)، ويستخدم هذا النظام زوجاً من المفاتيح (مفتاح عام (public key)، ومفتاح خاص ((private key) عوضاً عن استخدام مفتاح واحد فقط. ورغم أن هذا النظام كان ملائماً جداً لأجهزة الكمبيوتر المعقَّدة، إلا إنه قد تم اختراقه فيما بعد. وبقيت الحال على ذلك حتى قام فيل زيمرمان (Zimmerman Phil) عام 1986 بتطوير برنامج تشفير يعتمد نظام (RSA)، ولكنه يتميز باستخدام مفتاح بطول 128 بت، ويُدعى برنامج الخصوصية المتفوِّقة (Pretty Good Privacy- PGP). ويتوفر من هذا البرنامج نسخة تجارية و نُسخة مجانية، وهو من أكثر برامج التشفير انتشاراً في وقتنا الحالي.

4-5 ما هو التشفير (encryption)؟

يُعرَّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو

فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة. ومن المعلوم أن الإنترنت تشكِّل في هذه الأيام الوسطَ الأضخم لنقل المعلومات. ولا بد من نقل المعلومات الحساسة (مثل الحرَكات المالية) بصيغة مشفَّرة إن أُريدَ الحفاظ على سلامتها وتأمينها من عبث المتطفلين والمخربين واللصوص. وتُستخدَم المفاتيح في تشفير (encryption) الرسالة وفك تشفيرها (decryption). وتستنِد هذه المفاتيح إلى صِيَغ رياضية معقَّدة (خوارزميات). وتعتمد قوة وفعالية التشفير على عاملين أساسيين: الخوارزمية، وطول المفتاح (مقدَّرا بالبت (bits)). ومن ناحية أخرى، فإن فك التشفير هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك الشيفرة.



الشكل4-1 نموذج نظام تشفير اساسى

4-6 التشفير المتماثل(Symmetric Cryptography):

المفتاح السري (Secret Key) في التشفير المتماثِل، يستخدم كل من المرسِل والمستقبِل المفتاحَ السري ذاته في تشفير الرسالة وفك تشفيرها. ويتفق الطرفان في البداية على عبارة المرور (passphrase) (كلمات مرور طويلة) التي سيتم استخدامها. ويمكن أن تحوي عبارة المرور حروفاً كبيرة وصغيرة ورموزا أخرى. وبعد ذلك، تحوِّل برمجيات التشفير عبارةَ المرور إلى عدد ثنائي، ويتم إضافة رموز أخرى لزيادة طولها. ويشكِّل العدد الثنائي الناتج مفتاح تشفير الرسالة. وبعد استقبال الرسالة

المُشفَّرة، يستخدم المستقبِل عبارةَ المرور نفسها من أجل فك شيفرة النص المُشفَّر (cipher text or encrypted text)، إذ تترجِم البرمجيات مرة أخرى عبارةَ المرور لتشكيل المفتاح الثنائي (binary key) الذي يتولى إعادة تحويل النص المُشفَّر إلى شكله الأصلي المفهوم.

ويعتمد مفهوم التشفير المتماثِل على معيار DES. أما الثغرة الكبيرة في هذا النوع من التشفير فكانت تكمن في تبادُل المفتاح السري دون أمان، مما أدى إلى تراجُع استخدام هذا النوع من التشفير، ليصبح شيئاً من الماضي.

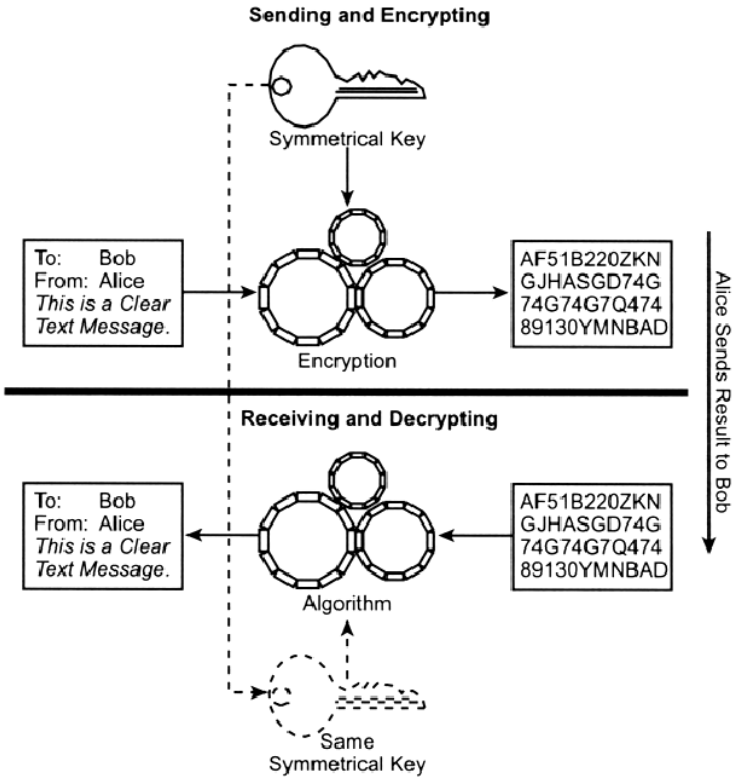


Exhibit 4-1. Symmetrical key encryption

7-4 التشفير اللامتماثل (Asymmetric Cryptography):

المفتاح العام (Public key) جاء التشفير اللامتماثل حلاً لمشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل، فعوضاً عن استخدام مفتاح واحد، يستخدِم التشفير اللامتماثِل مفتاحين اثنين تربط بينهما علاقة. ويُدعى هذان المفتاحان بالمفتاح العام (public key)، والمفتاح الخاص (private key). ويكون المفتاح الخاص معروفاً لدى جهة واحدة فقط أو شخص واحد فقط؛ وهو المرسِل، ويُستخدَم لتشفير الرسالة وفك شيفرتها. أما المفتاح العام فيكون معروفاً لدى أكثر من شخص أو جهة، ويستطيع المفتاح العام فك شيفرة الرسالة التي شفَّرها المفتاح الخاص، ويمكن استخدامه أيضاً لتشفير رسائل مالك المفتاح الخاص، ولكن ليس بإمكان أحد استخدام المفتاح العام لفك شيفرة رسالة شفَّرها هذا المفتاح العام، إذ إن مالك المفتاح الخاص هو الوحيد الذي يستطيع فك شيفرة الرسائل التي شفرها
المفتاح العام.

ويُدعى نظام التشفير الذي يستخدم المفاتيح العامة بنظام RSA، ورغم أنه أفضل وأكثر أمناً من نظام DES إلا إنه أبطأ؛ إذ إن جلسة التشفير وجلسة فك التشفير يجب أن تكونا متزامنتين تقريبا. وعلى كل حال، فإن نظام RSA ليس عصياً على الاختراق، إذ إن اختراقه أمر ممكن إذا توفَّر ما يلزم لذلك من وقت ومال. ولذلك، تمّ تطوير نظام PGP الذي يُعَدُّ نموذجاً محسَّناً ومطوَّراً من نظام RSA. ويستخدم PGP مفتاحا بطول 128 بت، إضافة إلى استخدامه البصمة الإلكترونية للرسالة (message digest). ولا يزال هذا النظام منيعاً على الاختراق حتى يومنا هذا

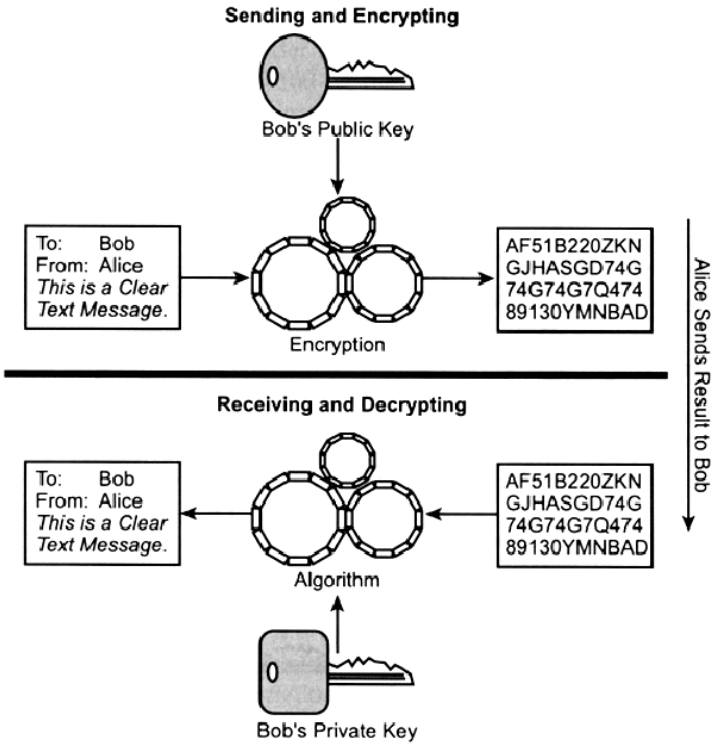


Exhibit 4-2. Asymmetrical key encryption

Hash Function 4-8

وظائفHash Functionوظائفَ حسابيةَ التي تَأْخذُ طولِ متغيرمِنْ البياناتِ كدخل وتنتج نتيجة ثابتة الطول الذي يُمْكِنُ أَنْ يُستَعملَ كبصمات إلاصابع لتَمْثيل البيانات الأصليه. لذا، إذا كان ال Hash لرسالتين مماثل،يُمْكِنُ أَنْ نفتَرضَ إلى حدّ معقول ان الرسائل ستكون مماثلة أيضاً.

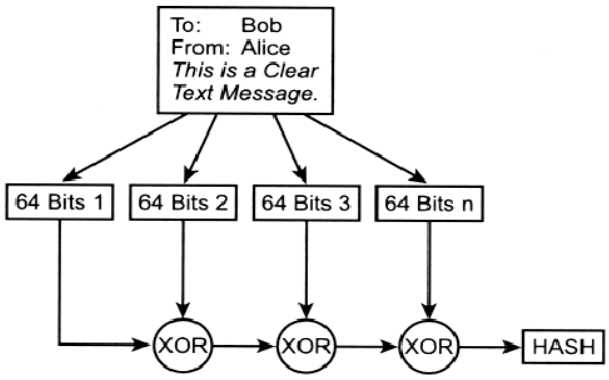


Exhibit 4-11. Simple hash function

Message Authentication Code 4-6:

هو عباره عن تشفير و hashing. كما بالشكل

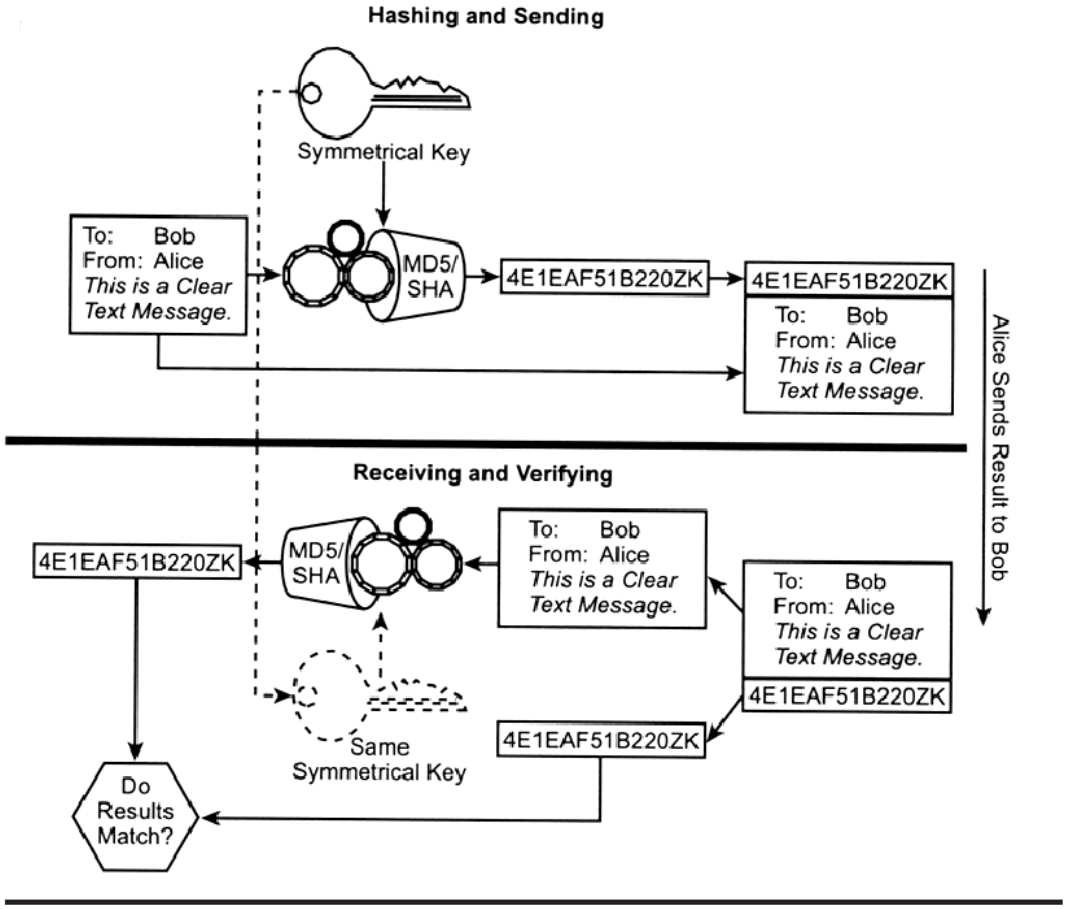


Exhibit 2-23. Message Authentication Code.

ان MAC جداً مشابه للتشفيرِ، لكن MACمُصَمَّمُ لِكي يَكُونَ غير قابل للنقضَ، مثلhash functionالمعيارة. بسبب الملكياتِ الحسابيةِ لعمليةِMAC، وعدم القابلية لعَكْس التشفيرِ المصمّمَ للعمليةِ،MACs أقل بكثيرعرضة للهجماتِ مِنْ التشفيرِ بنفس الطولِ الرئيسيِ. يَضْمنُ MAC سلامةَ البياناتَ كبتات لكن المُستلمَ يَجِبُ أَنْ يكونَ عِنْدَهُ المفتاح السِرّي المشترك لإنْتاج نفس MAC لتَصْديق الرسالةِ.

Hash-based message authentication code HMAC

Hashed-based message authentication code (HMAC) is the process of combining existing cryptographic hashing functions with a key.

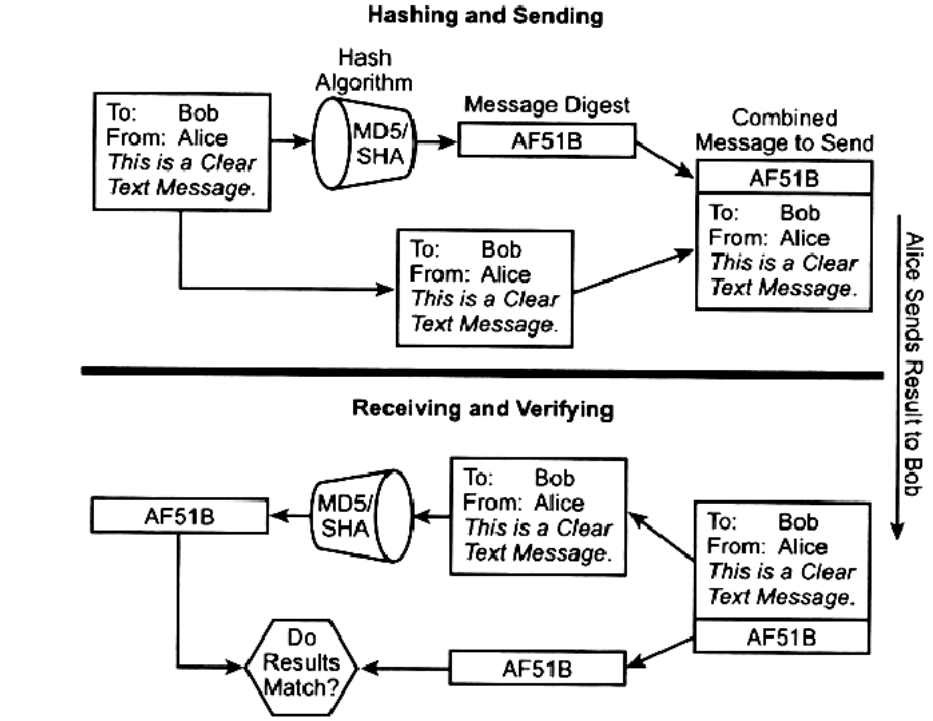


Exhibit 4-8. Hash function

لكن لا تزال هنالك مشكلتان في ذلك:

المشكلة الأولى هي أن تشفير البيانات باستخدام أسلوب التشفير بالمفتاح الغير متناظر عملية معقدة ترهق معالج الكمبيوتر وتستغرق الكثير من الوقت، لذا فإنها غير عملية لتبادل رسائل طويلة نسبيا، والحل لهذه المشكلة يكمن في استخدام الأسلوب الأسرع في التشفير وهو أسلوب التشفير بالمفتاح المتناظر.

قلنا سابقا بأن مشكلة التشفير بالمفتاح المتناظر هي عدم وجود طريقة آمنة وعملية لنقل المفتاح الذي يستخدم لتشفير البيانات وفك تشفيرها عبر الشبكة، لكن الآن بفضل التشفير بالمفتاح الغير متناظر فإن ذلك أصبح أمرا سهلا.

ما ستقوم به المواقع الآن هي أنها بعد تتبادل مع المتصفح المفاتيح العلنية، فإنها لن تستخدم هذه المفاتيح لتشفير البيانات نفسها، بل ستستخدمها لتشفير مفتاح التشفير

الذي سينتج عشوائيا لهذه العملية وسيتم تغييره الآن بصفة دورية أثناء الاتصال بين المزود والزبون.

أما البيانات نفسها التي سيتم تبادلها فسيتم تشفيرها باستخدام التشفير المتناظر، أي باستخدام خوارزميات مثل DES وAES.

المشكلة الثانية في نظام التشفير هذا هي أنه لا يزال قابلا للاختراق بسهولة باستخدام هجوم يدعى هجوم الرجل الذي في الوسط (Man in the middle attack).

قلنا قبل قليل بأننا عندما نقوم بزيارة واحدة من المواقع الآمنة فإننا نستقبل منها مفتاحها العمومي لنتمكن من تشفير البيانات الحساسة وإعادة ارسالها إلى الموقع، لكن المشكلة التي تطرح نفسها هي: ما الذي يضمن لك بأن الذي أرسل لك هذا المفتاح العمومي هو الموقع الذي تريد التعامل معه؟

ما يحدث في هذا النوع من الهجمات هو أن المخترق يقوم باعتراض الاتصال بينك وبين المزود، بحيث يأخذ البيانات التي أردت ارسالها منذ البداية من جهازك إلى المزود ويرسلها هو إلى المزود من جهازه هو، فيعتقد المزود بأنك موجود على جهاز المخترق، وفي نفس الوقت، يقوم المخترق بالرد عليك ويرسل إليك المفتاح العلني الخاص به، بدلا من أن تحصل على المفتاح العلني الخاص بالمزود الحقيقي الذي تريد التعامل معه، وعندما تقوم بتشفير البيانات بالمفتاح العلني للمخترق، فإنه سيتمكن من فك تشفيرها باستخدام المفتاح الخاص به، وبعد ذلك.

كما أنك عندما تحاول ارسال المفتاح العلني الخاص بك إلى المزود، فإن المخترق سيأخذ هذا المفتاح ويحفظ به عنده ويرسل بدلا منه المفتاح العلني الخاص به إلى المزود، وبالتالي فإن المزود سيشفر البيانات بالمفتاح العلني الخاص بالمخترق أيضا وبالتالي فإن المخترق سيتمكن من فك تشفيرها باستخدام مفتاحه الخاص، وبعد ذلك يقوم بتشفيرها بمفتاحك العلني وارسالها إليك حتى تشعر بأن الاتصال يتم بصورة

صحيحة مع المزود، لكن ما يحدث في الواقع هو أن المخترق يقوم بإدارة اتصالين مشفرين منفصلين، الاتصال الأول بينك وبينه، والاتصال الثاني بينه وبين المزود، وبين هذين الاتصالين تكون البيانات غير مشفرة، وبذلك يحصل على ما يريد، وهو التنصت على المعلومات المتبادلة بينك وبين المزود.

ويمكنك أن تقول بعبارة أخرى بأنه ينتحل شخصية المزود بالنسبة للزبون وينتحل شخصية الزبون بالنسبة للمزود، فيتوهم الطرفان بأنهما يتخاطبان مباشرة مع بعضها البعض دون أن يعلما بأنها في الواقع يتخاطبان مع جهاز المخترق، وفي أثناء ذلك فإن المخترق يحصل على كافة المعلومات الغير مشفرة بكونه يلعب دور الوسيط بينهما، ولهذا السبب سمي هذا الاختراق باختراق الرجل في المنتصف أو الرجل الوسيط.والحل لهذه المشكلة يكون باستخدام أمر يسمى الشهادات الالكترونية، وهي أيضا تعتمد على تقنية التشفير بالمفتاح العلني.

6-5 توثيق صحة البيانات ومصدرها (التوقيع الالكتروني والشهادات الالكترونية):

كما كنت أقول قبل قليل، التبادل الالكتروني الآمن على الانترنت يتطلب وجود طريقة نتأكد منها من شخصية الطرف الذي نتصل به ومن أن الرسائل التي نستقبلها منه قادمة بالفعل منه وأنها ليست رسائل مزورة، والتقنية المستخدمة لتحقيق ذلك تسمى التوقيع الالكتروني (Digital Signing).في التوقيع الالكتروني، يقوم المزود الذي سيقوم بإرسال رسالة ما للزبون (بغض النظر عن حالة الرسالة من حيث كونها مشفرة أو لا) بتشفير هذه الرسالة النهائية مرة أخيرة باستخدام المفتاح الخاص به، وعندما تصل الرسالة إلى الزبون فإنه يقوم بفك تشفيرها باستخدام المفتاح العلني للمزود، فإذا نتج عن فك تشفير هذه الرسالة النتيجة التي يتوقعها الزبون فإنه يعلم بأن المزود هو بالفعل مصدر هذه الرسالة.

فلاحظ هنا بأننا نقوم بعملية عكسية، فبدلا من أن نشفر الرسالة بالمفتاح العلني ونرسلها للمزود، بحيث لا يتمكن أحد من فكها إلا المزود، فإن المزود يقوم هو بتشفيرها بمفتاحه الخاص ويرسلها إلى الزبون، بحيث يتمكن أي شخص من فك

تشفير الرسالة باستخدام المفتاح العلني للمزود، لكن المزود وحده فقط يكون قادرا على تشفيرها باستخدام المفتاح الخاص لأنه وحده الذي يملك المفتاح الخاص، وبالتالي نكون متأكدين من أن الرسائل التي تقبل فك التشفير باستخدام المفتاح العلني للمزود هي رسائل مرسلة من المزود نفسه.

ونلاحظ أيضا بأن الرسائل في هذه الحالة تكون عادة مشفرة مرتين :

في المرة الأولى تشفر الرسالة الأصلية المحتوية على المعلومات الحساسة بالمفتاح العلني للزبون حتى لا يتمكن أحد من فك تشفيرها سوى الزبون، وتشفر بعد ذلك هذه الرسالة المشفرة نفسها مرة أخرى باستخدام المفتاح الخاص للمزود ليثبت للزبون بأنه هو الذي قام بارسال الرسالة وذلك بأنها تقبل فك التشفير بالمفتاح العلني للمزود.

وكما شرحت سابقا فإن هذه العملية تتم في بداية الاتصال فقط للاتفاق على مفتاح متناظر مؤقت ليستخدم مع البيانات الفعلية للاتصال لتسريع الأمور.لكن تظل هنا مشكلة أخيرة بحاجة للحل،

وهذه المشكلة هي أننا قلنا بأن المزود سيقوم بتشفير الرسائل باستخدام مفتاحه الخاص وأن كون هذه الرسائل قابلة للفك باستخدام المفتاح العلني للمزود هو الدليل على أنها صادرة من المزود

لكن ما الذي يضمن بأن هذا المفتاح العلني هو المفتاح الصادر من المزود أصلا؟ وأنه ليس مفتاحا لمخترق وضع نفسه في منتصف الطريق بينك وبين المزود؟

هنا يأتي دور الشهادات الالكتروني (Digital Certificates)، وهذه الشهادات هي عبارة عن رسالة تقول بأن الجهة الفلانية مثلا تشهد بأن المفتاح العلني للمزود الفلاني هو كذا.

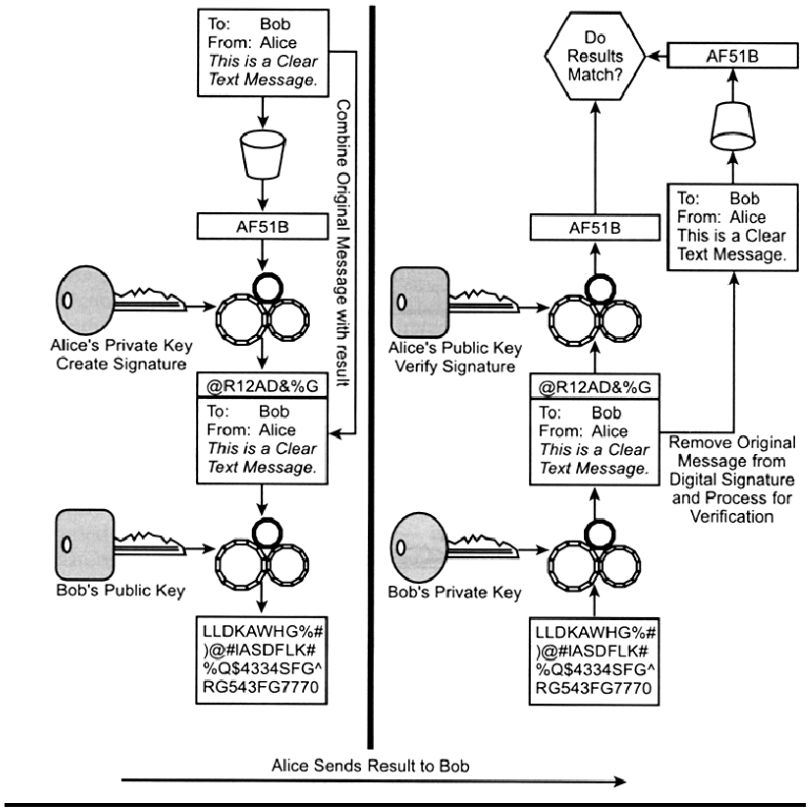


Exhibit 4-3. Digital signature with the use of hash functions

مما سبق نستنتج انه بامكاننا اختيار نوع التشفير الذى نريده حسب درجه السرية والامن الذي نريدة لتحقيق VPN وكذلك نختار الخوارزمية المناسبة للتشفيروالتى اشهرها

DES, 3DES, RC5, IDEA, CAST, BlowFish, 3IDEA,RSA

الفصل الخامس

الأنفاق و بروتوكولات الشبكة الخاصة الافتراضية

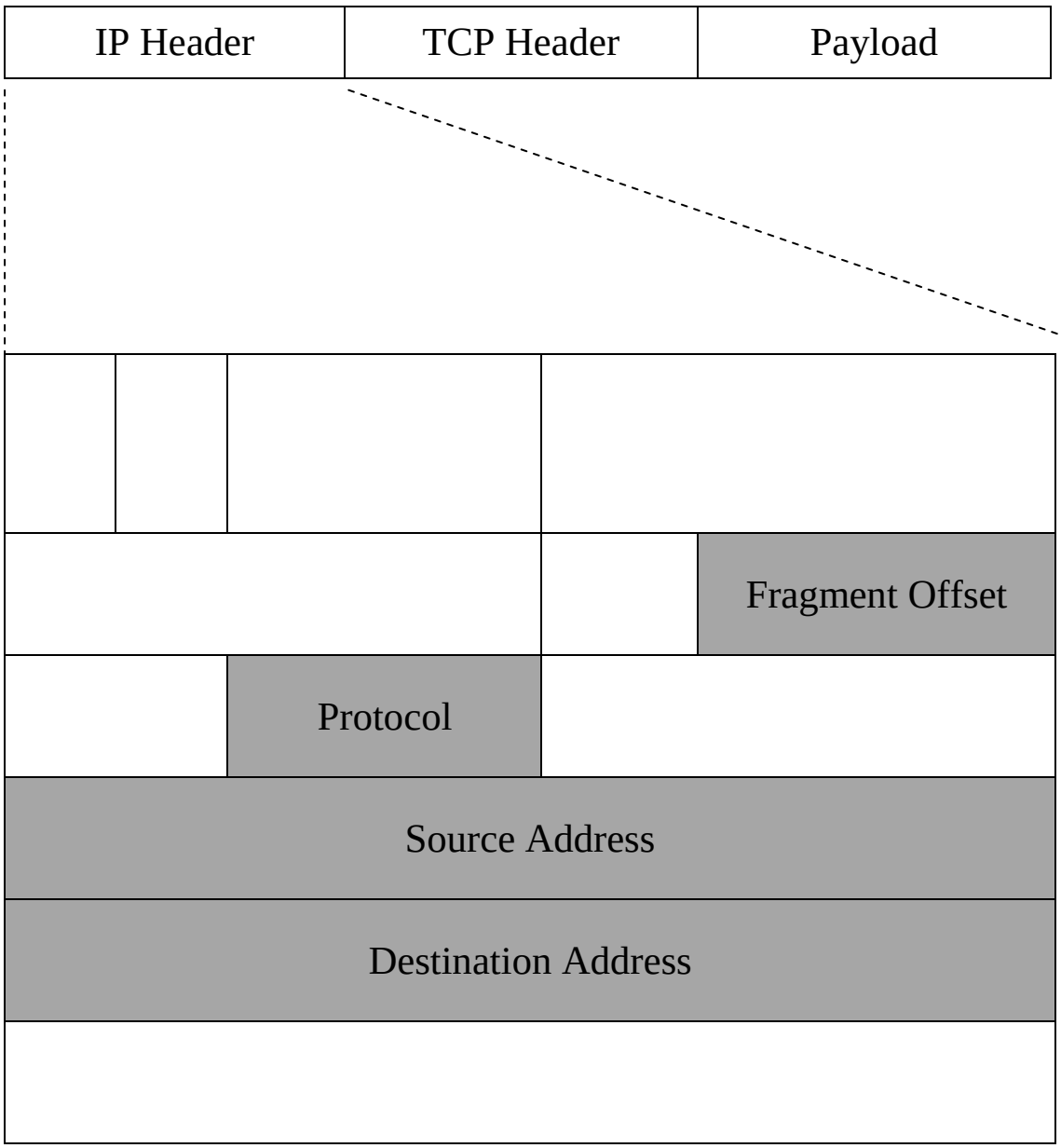
تستخدم الشبكات الافتراضية الخاصة في عملها عدة بروتوكولات ,سواء في التشفير أو التوثيق أو الأنفاق عبر الشبكة العامة ,سنوضح في هذا الفصل آلية عمل هذه البروتوكولات معاً. بداية مع الأنفاق التي تعتبر مسؤولة عن تأسيس الاتصال ثم ننتقل إلى محددات هذا الاتصال التشفير و التوثيق و التحكم بالوصول.

5-1 الأنفاق:

هي التقنية التي استدعت وجود كلمة افتراضية في تسمية VPN و هي التي تسمح باستخدام شبكة الانترنت أو الشبكات العامة الأخرى لإرسال البيانات أو بكلمة أوضح فإن الأنفاق تغلف البيانات بترويسات جديدة بحيث تخفي الترويسات الأصلية عن وسط النقل المستخدم.باستخدام الترويسات الجديدة تقوم أجهزة الشبكة بتوجيه الرزم عير الانترنت إلى هدفها المرحلي ريثما تزال هذه الترويسات و تعود الرزمة إلى وضعها الأصلي.

5-2 تغليف IP Packets:

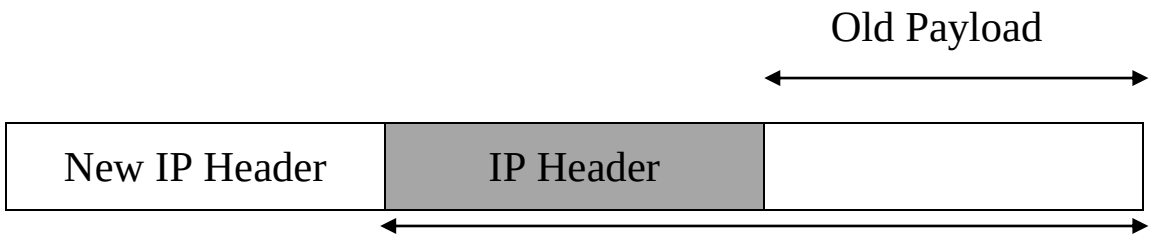
لنشرح بدايةً ترويسة الرزمة في IPv4.يوضح الشكل التالي بنية هذه الترويسة التي تتألف من قطاعات ثابتة البنية :



3-5 بناء النفق:

عندما نستخدم بروتوكولاً لبناء نفق مثل IP Sec فإننا نلحق بالرزمة ترويسة IP جديدة بحيث تعدل فيها الحقول الرمادية في الشكل السابق بحيث تصبح كما يلي:
حقل البروتوكول يحدد البروتوكول المستخدم في الطبقة التالية و هو بالشكل الطبيعي قد يكون TCP,UDP,ICMP. أما عند تطبيق IP Sec فإن هذا الحقل سيتغير ليشير إلى وجود بروتوكول مغاير في الطبقة الأعلى و هو ترويسة IP الأصلية.

أما حقل الإزاحة يتضمن مقدار انزياح البيتات عن بداية الترويسة IP و سيتعرض هذا الحقل للتعديل ليشير إلى القيمة الجديدة نتيجة لتغير الإزاحة بعد تغير الترويسة:



تتعامل الموجهات في الانترنت مع هذه الترويسة الجديدة لتوجيه الرزمة كما يجب القول أن الرزمة القديمة (بداية من ترويسة IP الأصلية و حتى نهاية الرزمة) يتم ضغطها و تشفيرها من ثم تلحق بها هذه الترويسة الجديدة.

إن الرزمة الأصلية قد تعتمد بروتوكولات أخرى مغايرة لـ IP (مثل IPX) و بالتالي فإن عملية التغليف تسمح بنقل هذه الرزم مع أنها تعتمد بروتوكولات غير قابلة للتوجيه .

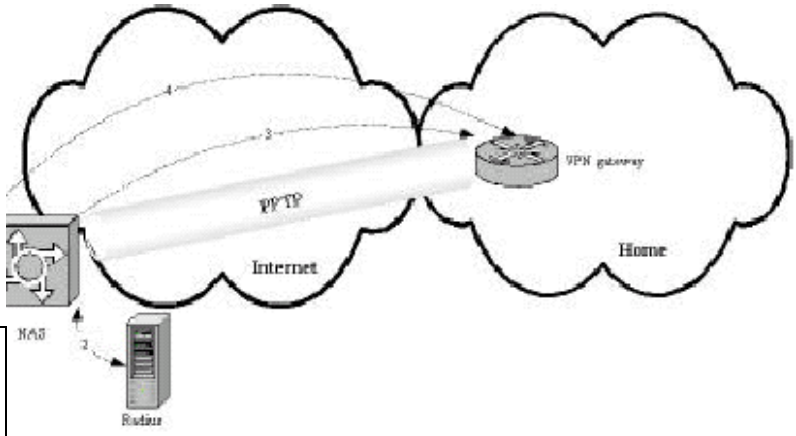
-هناك حالة خاصة بالنسبة لـ IP لا يمكن نقلها عبر الانترنت و هي عناوين البث العام (Broadcast) و ذلك لأن الموجهات تسقط الرزم الحاوية على مثل هذه العناوين.

من الواضح أن عملية إنشاء الأنفاق تشير إلى حد بعيد إلى عملية الكبسلة أنفة الذكر. إلا أن المصطلح (Encapsulation) لا يشير تماماً إلى النفق لأن النفق في واقع الأمر هو عبارة عن حزمة من الاتصالات التي تعبر الانترنت بين مصدر و هدف معينين و هكذا فإن ربط شبكتين باستخدام نفق يعني أن عدة مستخدمين في كل شبكة يستخدمون هذا النفق في الوقت نفسه.

4-5 أنفاق PPTP:

يبدأ الزبون باتصال هاتفي باستخدام PPTP(Point to-Point Protocol) إلى مخدم(Network Access Server) NAS يدعم خدمة PPTP.

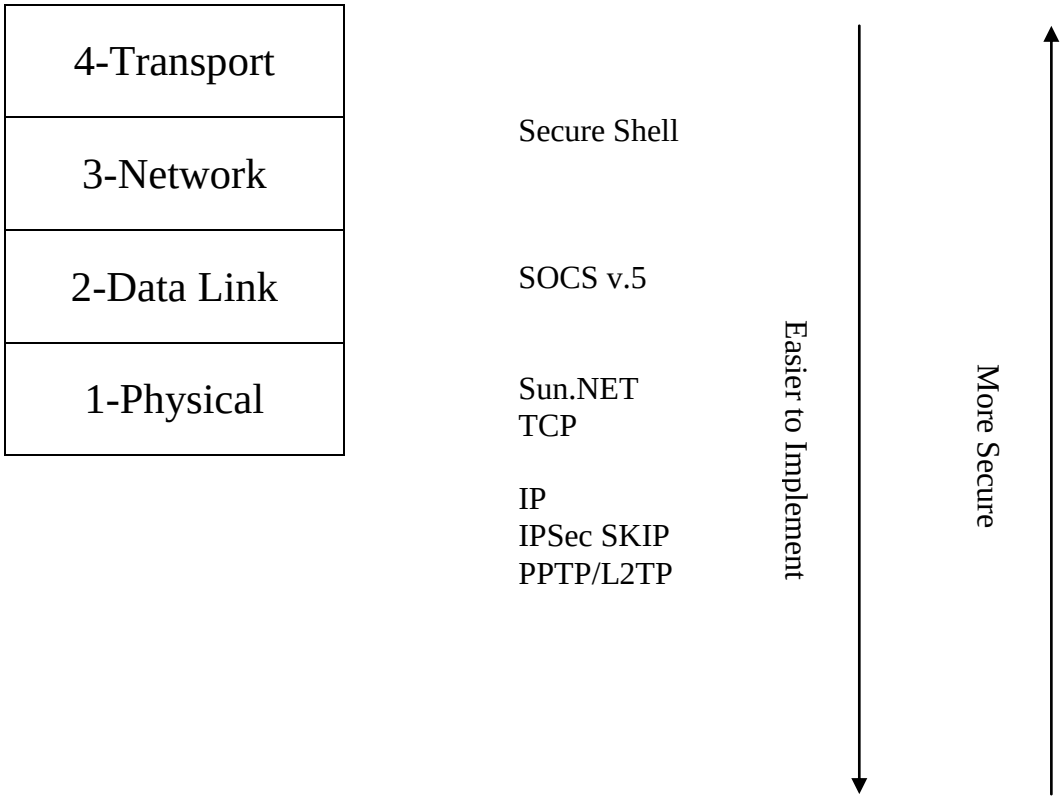
عندما تنتهي هذه الخطوة يقوم NAS بفتح اتصال ثان عبر شبكة الانترنت إلى مخدم VPN مستخدماً PPTP و عبر هذا الاتصال يقوم NAS بتوثيق المستخدم عند VPN لضمان شخصية المتصل. بعد هذه المرحلة فإن النفق المنشأ جاهز لنقل الرزم المغلفة ببروتوكول PPTP بشكل آمن بين المستخدم و الشبكة الواقعة خلف مخدم VPN.



7-Application
6-Presentation
5-Sission

Packet-Oriented VPN 5-6:

إن التركيز في صناعة VPN ينصب حالياً على PO-VPN و التي تعمل في الطبقة الثانية أو الثالثة في نموذج OSI المرجعي:



نموذج OSI المرجعي و توضعات بروتوكولات VPN

5-7 PPTP(Point-to-Point Tunneling protocol):

يعتبر هذا البروتوكول بروتوكولاً موسعاً من البروتوكول PPP المستخدم للاتصال بالإنترنت عبر الطلب الهاتفي .

طور PPTP من قبل Ascend Communications,Microsoft,3Com .

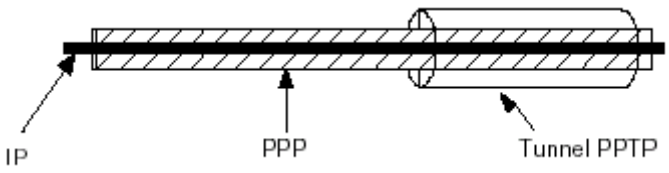
و ضمن لأول مرة في Windows NT 4.0 و Win98.إلا أن مسودات IETF حول PPTPلم تحدد صراحة آلية التوثيق و التشفير المستخدمة لذا فإن المنتجات من مصنعين مختلفين قد لا تتوافق مع بعضها البعض.

في الحالة العامة يقوم PPTP بضغط و تشفير رزم PPP لنقلهم عبر الانترنت.إن عملية النقل هذه تستوجب و جود ترويسة IP و يتم تشكيل هذه الترويسة باستخدام نسخة معدلة من GRE(Generic Routing Encapsulation) .

عند المستقبل يقوم PPTP المناظر بنزع ترويسة IP و من ثم يفك تشفير رزمة PPP و يفك ضغطها ليحصل على الرزمة كما تم إرسالها من قبل المصدر.

يستخدم PTPP منفذ TCP رقم 1723 و معرف بروتوكول IP رقم 47 وذلك بناءاً على قرار هيئة LANA(Internet Assigned Number Authority) و بذلك يمكن لرزم PPTP المرور عبر الموجهات و الجدر النارية بعد إعدادها للسماح للحركة التي تستخدم هذه المنافذ أي أن مخدم VPN أن يركب خلف الجدر النارية.

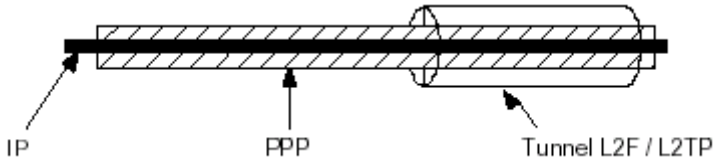
نسخة Microsoft من PPTP و المضمنة مع نظم تشغيل Windows تعتمد على خوارزمية DES للتشفير المتناظر و يتم اشتقاق مفتاح التشفير من كلمة المرور التي يوثق بها المستخدم لدى مخدم VPN.يعتبر هذا النموذج لتوليد المفتاح ثغرة أمنية لكونه يعرض كامل الجلسة لخطر الاختراق بمجرد معرفة كلمة السر.



5-8 L2FP(Layer 2 Forwarding Protocol):

تم تطوير L2FP من قبل شركة Cisco ويعمل هذا البروتوكول في الطبقة الثانية في نموذج OSI المرجعي . فضلاً عن تضمينه مع منتجات Cisco فقد دعمت Northern Telecom و Shiva Corporation بروتوكول L2F.ما يميز هذا البروتوكول أنه ليس محصور بشبكة الانترنت مثل PPTP بل يستطيع العمل في شبكات ATM.

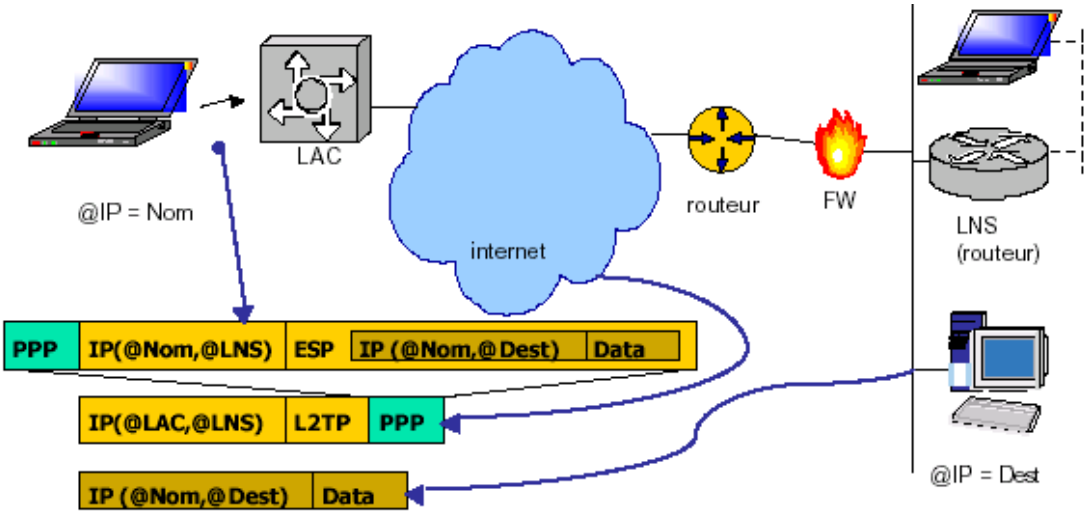
و عندما قدمت Cisco معيار L2FP لهيئة ITEF قامت الأخيرة بدمجه مع بروتوكول PPTP الذي قدمته Microsoft و كانت النتيجة هي L2TP(Layer 2 Tunneling Protocol).



5-9 L2TP(Layer 2 Tunneling Protocol):

كما سلف الذكر فإن IETF قامت بتوقيع أول مستند يوصف L2TP و كانت مجموعة العمل التي شكلتها الهيئة مؤلفة من Cisco و Microsoft و Ascend و3COM و US. Robotics و ضمن هذا البروتوكول بداية مع Win NT 5.0.

كما هو الحال مع PPTP يقوم L2TP بنقل الرزم غير المعتمدة على IP مثل IPX و Apple Talkبالإضافة إلى رزم IP الاعتيادية كما و يستطيع L2TP بتأسيس اتصال VPN عبر الشبكات المغايرة للانترنت مثل ATM و Sonet.



5-10 IP sec:

IP sec هو امتداد لبروتوكول الانترنت مع إمكانيات ضخمة لحماية البيانات على مستوى IP مع توثيق المستخدمين و نظام تشفير حيث أن IP sec هو عبارة عن مجموعة من البروتوكولات التي تتعاون مجتمعة لتقوم VPN على أتم وجه.

بنية رزمة IP sec:

تبدأ رزمة IP sec بترويسة IP التقليدية مما يعني أنه بروتوكول قابل للتوجيه عبر الانترنت باستخدام المعدات نفسها التي تستخدم لنقل الرزم العادية.يحوي حقل معرف البروتوكول رقماً يدل على أنه هناك بيانات مشفرة في الطبقة الأعلى خلافاً لـ IP الذي يدل على TCP أو UDP غالباً.

ترويسة التوثيق (AH) تسمح لمستخدمي IP sec أن يتأكدوا من وصول البيانات دون تعديل و دون أي تدخل من طرف ثالث غير المرسل و المستقبل .

الحمل الأمن المشفر (ESP) يحمل هذا القطاع من الرزمة البيانات بالإضافة إلى بروتوكول الطبقة الأعلى الأساسي (TCP مثلاً) في صيغة مشفرة.

نتيجة:

عرض هذا الفصل البروتوكولات و الخوارزميات المستخدمة في بناء VPN .و مما يجب ملاحظته أن هذه البروتوكولات – مع إمكانية عملها بشكل مستقل– في بعض الحالات قد تعمل بشكل مشترك لتحقيق أمان أعلى لـ VPN فمثلاً قد يستخدم IP sec مع L2TP بحيث أن L2TP مسؤول عن بناء النفق و IP sec يهتم بباقي الوظائف من توثيق و تشفير.

الآن وقد شكلنا فكرة جيدة عن VPN و الخيارات المتاحة فقد حان الوقت لنبدأ بدراسة بنى الـ VPNلاتخاذ القرار حول أفضل نموذج لاستخدامه و مجالات استخدام كل نموذج.

الفصل السادس

بنية الشبكة الخاصة الافتراضية

إن بنية VPN محكومة بما تريد من VPN أن تقدم لك فيما إذا كنت تريد استثمارها لخدمة القوة المتنقلة أو لتصل مكاتب الشركة ببعضها .كما أن متطلبات VPN قد تختلف فيما لو كنت تبني إنترانت أو إكسترانت , و يلعب العامل الأمني دوراً في تحديد البنية و عملية توزيع التجهيزات .

من وجهة النظر الفيزيائية فإن أهم العوامل المؤثرة في القرار هي أين يبدأ النفق و أين ينتهي و على أي مستوى نطبق التشفير و أين تقع مخدمات VPN نسبةً للتجهيزات الأخرى و بكلمة مختصرة أين تبدأ VPN و أين تنتهي.

6-1 الحلول البرمجية و الحلول العتادية:

باستثناء القوة المتنقلة فإن أي سيناريو يمكن أن يستخدم لبناء VPN مع و ظائف الأنفاق و التشفير مطبقة عبر عتاد صلب أو عبر حزمة برمجية على كمبيوتر أغراض عامة .

لو أخذنا الحل البر مجي بداية فإن تحميل الحزمة على جهاز يعمل كمخدم أو جدار ناري لا يعتبر من الحكمة بمكان لان الأداء العام لهذا الجهاز سيتدهور بشكل كبير بشدة وذلك لأن التشفير

- الأساسي بالنسبة لـ VPN- يستهلك موارد الجهاز بشراهة لأنه يتطلب عمليات حسابية معقدة و هذا ما يحجز المعالج لفترة طويلة .

إذا فإن VPN تتطلب جهازاً متفرغاً للعمل و مجهز بمعالج سريع و ذوا كر متخصصة ليكون قادراً على تنفيذ وظائف VPN بأداء عالي .

يقدم الحل البر مجي ميزة لا يقدمها الحل العتادي و هي المرونة العالية فعند ازدياد الضغط على الشبكة و تراجع أداء VPN تستطيع بكل بساطة أن تستبدل الكمبيوتر بآخر ذي مواصفات أعلى ليتعامل مع الإحداثيات الجديدة للوضع الأمر الذي يبقى ضمن الحدود المعقولة للكلفة حيث تستطيع إعادة الجهاز القديم ليعمل في وظيفة أخرى.

أما بالنسبة للحل العتادي فهناك شرائح متاحة عالمياً مصممة لتقوم بعمليات التشفير و الضغط.

إن هذا العتاد يقدم أداء أعلى بكثير من الحلول البرمجية. و يبقى من المكلف تطوير مثل هذه المعدات بعد تركيبها إذ أنه من الواجب تبديل الجهاز بالكامل و بالتالي ماذا نفعل بالجهاز القديم؟.

6-2 إخفاء الشبكة:

من أهم العوامل التي يجب مراعاتها عند تصميم الـ VPN هو إخفاء الشبكة خلف VPN عن الانترنت, تقدم بروتوكولات VPN هذه الميزة عبر عملية تغليف الرزم الأصلية بترويسات جديدة تخفي العناوين الأصلية و تستبدلها بعناوين طرفيات VPN في الترويسات الجديدة.

من المعلومات المفضلة لدى قراصنة الشبكة هي العناوين حيث بمعرفة عنوان جهاز مخدم يستطيعون القيام بكثير من العمليات المؤذية بعد الالتفاف حول الجدار أو الناري فكلما قلت معرفتهم حول تفاصيل الشبكة الداخلية ضمنت ارتفاع أمن شبكتك إلى حد يجعل الأعباء الإدارية المضافة في عملية إخفاء العناوين مهملة أمام ارتفاع المستوى الأمني للشبكة.

6-3 توثيق المستخدمين:

بالإضافة إلى VPN نفسها فإن توثيق المستخدمين هو واحد من التحديات المطروحة أمام بنية الـ VPN و يلعب توضع المستخدمين دوراً هاماً في التخطيط لبنية الشبكة من حيث موقع مخدم التوثيق و قاعدة بيانات المستخدمين و حجم VPN ذاتها.

VPN صغيرة الحجم تعمل كإنترانت فإن قاعدة بيانات المستخدمين المحلية كافية لتخديم كامل الشبكة أما مع ازدياد حجمها وانتقالها إلى إكسترانت تظهر من أجل التعقيدات من الممكن في هذه الحالة استخدام مخدم راديوس.

في شبكات VPN عالية الضخامة فإن الخيار الوحيد المتاح هو المعايير الصناعية الضخمة مثل OASIS التي تم فيها استخدام مخدمات RADIUS عالية الكفاءة.

النماذج الأساسية: بشكل أساسي إن لم تكن كل أنظمة VPN فإن معظمها مزيج من نموذجين أساسين :الأول زبون إلى شبكة و الثاني شبكة إلى شبكة.

بشكل إن لم تكن كل أنظمة VPN فإن معظمها مزيج من نموذجين أساسيين

الأول زبون– إلى - شبكة والثاني شبكة – إلى– شبكة

الفرق بين هذين النموذجين ليس كبيراً إنما توجد اعتبارات تفرق بينهما ففي **نموذج شبكة إلى شبكه:**

يوجد لدينا بنيتان فرعيتان هما انترانت و إكسترانت

إن العامل الأساسي في التمييز هو المكان الذي ينجز فيه عمل VPNوأين ينتهي النفق وغالباً ما يلعب الجدار الناري دوراً في تحديد هذا العامل.

زبون– إلى– شبكة:

من أكثر الأمثلة شيوعاً على هذا النموذج هو اتصال القوة العاملة المتنقلة بشبكة الشركة عبر RSA سنناقش الآن طرف الزبون فقط لأن الطرف الثاني من جهة الشبكة مطابق تماماً للنموذج الثاني شبكة–إلى–شبكة.

النمط الأول للنفاذ عن بعد للنفق المؤسس من قبل المستخدم أو خدمة الأنفاق المستقلة .

في هذا النمط يقوم المستخدم بتأسيس الاتصال إلى الانترنت عبر طلب هاتفي من خلال مزود الخدمة المحلي المجهز بمخدم NAS يعمل برنامج VPNعلى جهاز المستخدم المحمول و يقوم بتشفير البيانات و تشكيل النفق عبر الاتصال السابق لتصل البيانات إلى هدفها الأخير.

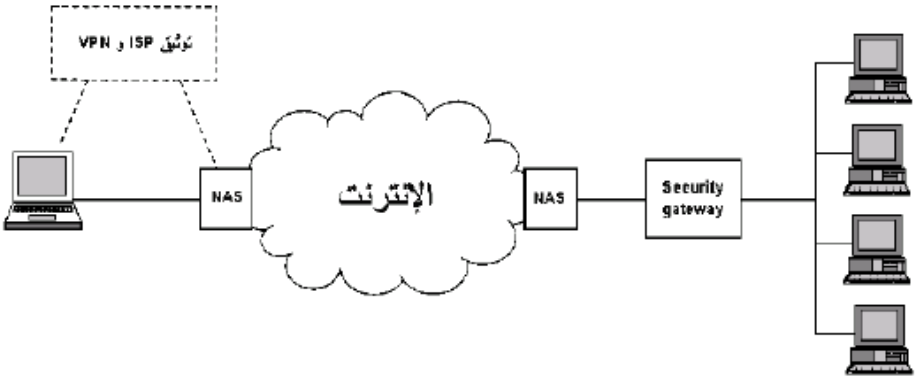
من أشهر الأمثلة على هذا النمط بروتوكول PPTP المعتمد من قبل Microsoft يعاني هذا السيناريو من سلبية كبيرة و هو أنه يضع كامل العبء على جهاز المستخدم ممايعني تراجعاً في الأداء إلى حد غير مقبول كون المعالج قد يبقى فترة

بيانات تنتقل عبر اتصال هاتفي بطيء و من ثم يقوم طويلةً نسبيا في انتظار معالجة هذه البيانات لمدة لا يستهان بها لتعود إلى وضعها الطبيعي .

النمط الثاني لنموذج زبون– إلى – شبكة هو المسمى النفق المؤسس من قبل NAS في هذه الحالة كما نلاحظ في الشكل فإن النفق محصور ما بين NAS المحلي و NAS البعيد أما وصلة NAS-مستخدم فلا تعتمد الأنفاق.

في هذا السيناريو يقوم المستخدم بتأسيس اتصال طلب هاتفي إلى مزود الخدمة و يوثق نفسه لدى هذا المزود الذي بدوره يقوم ببناء النفق باتجاه VPN التي يطلبها المستخدم.

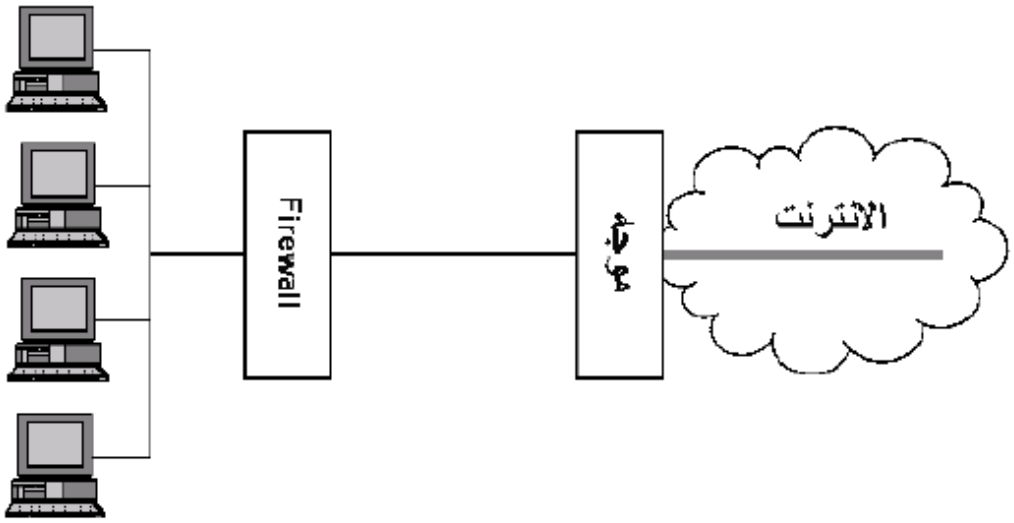
إن مزود الخدمة في هذه الحالة هو نقطة النهاية للنفق و عنده تتم عمليات التشفير وفك التشفير الأمر الذي يخفف إجهاد جهاز المستخدم . يسبب هذا النمطً إرباكا لمدراء الشبكة لأن عليهم الاتفاق مع مزودات الخدمة على هذه العملية و تزويدها بهويات المستخدمين المرخصين للوصول إلى VPN .



الشكل 7-2 النفق المؤسس من قبل NAS

نموذج شبكة إلى شبكة:

عند استخدام VPN لوصل شبكتين فإن الأنفاق بين الشبكتين ستبقى قائمة بشكل مستمر و تستدعي تعقيدات أكبر مما لو كان الاتصال عبر طلب هاتفي مؤقت.



الشكل 7-3 *Router-terminated VPN*

إن هذا النموذج يتطلب موجهات أو جدر نارية و بالتالي يظهر السؤال أين يبدأ اتصال VPN بالنسبة للموجه و بالنسبة للشبكة نفسها و أين ينتهي .

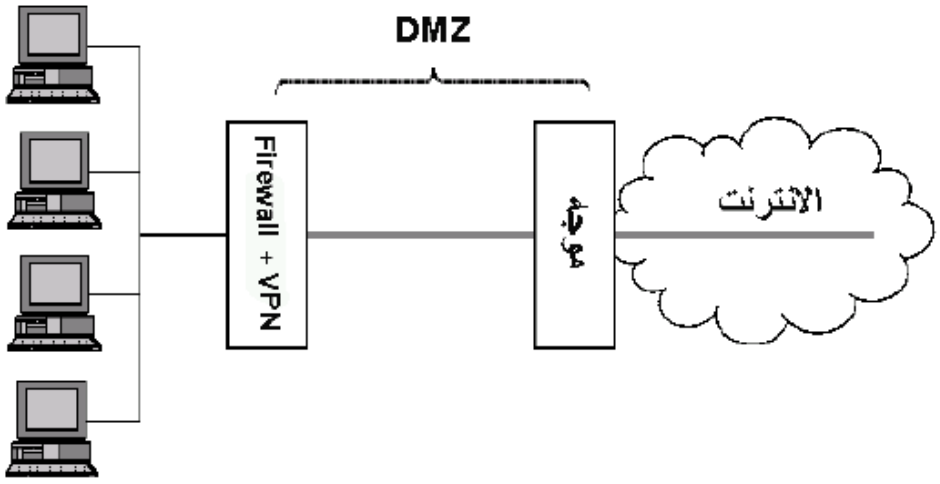
قبل أن نستعرض الخيارات المتاحة ينبغي القول أن البنية في طرفي اتصال VPN قد تكون

متباينة فلا وجوب لتطابق توزيع التجهيزات لذلك فإن عرض طرف واحد يكفي لتوضيح الفكرة.

Router-terminated VPN 6-4

يعتبر هذا السيناريو الأشهر حاليا, هذه الإعدادات تقدم جملة من المزايا حيث يقوم بكافة عمليات الأنفاق والتشفير و فك التشفير و من الواجب في هذه الحالة أن يكون الموجه قادراً على التعامل مع هذا الحمل.

Firewall VPN 6-7:



الشكل 7-4 *Firewall VPN*

إن الاتصال التقليدي بين شبكة محلية و شبكة الانترنت يستدعي وجود جدار ناري من جهة الشبكة و موجه من جهة الانترنت و المنطقة بين هذين الجهازين تدعى بالمنطقة منزوعة

DMZ (De-Militarized Zone) و هنا لدينا احتمالان في توظيف VPN:

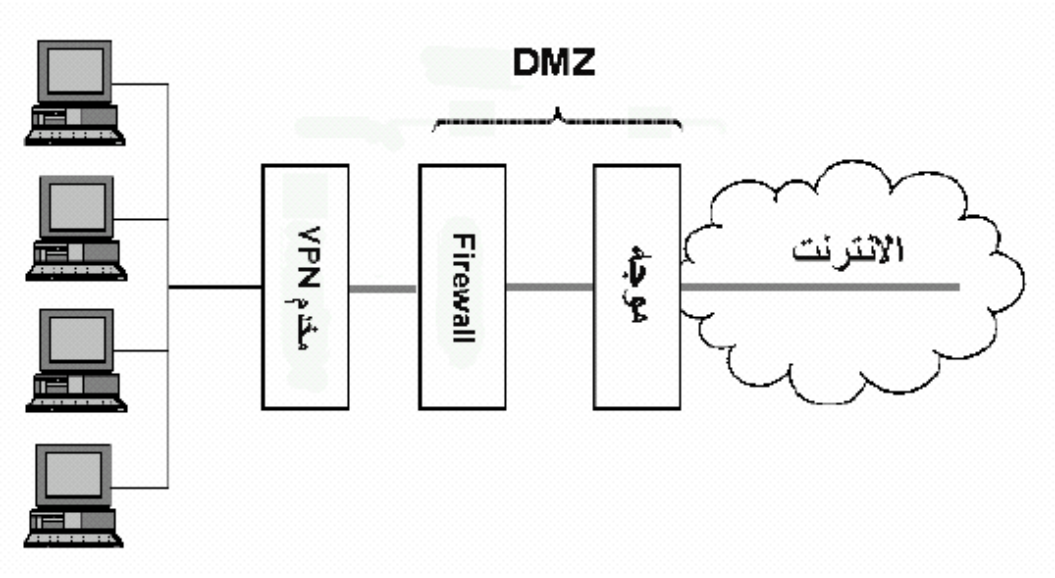
السلاح

الاحتمال الأول و هو VPN مع جدار النار حيث أن الحركة في الشبكة الداخلية بتضمين تشفر عبر الجدار الناري و من ثم يؤسس النفق عبر الموجه و فيه تمر هذه الحركة .

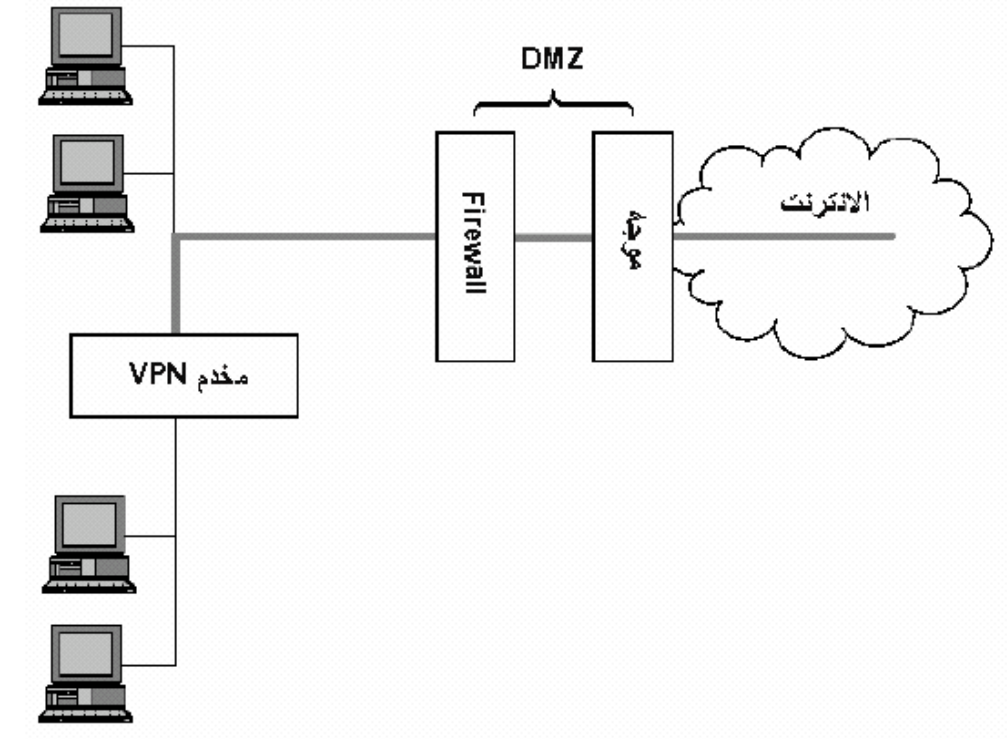
مرة أخرى يكون الحمل مركزاً على جهاز وحيد هو الجهاز الناري الذي سيكون أساسا محملاً بما فيه الكفاية .

الاحتمال الثاني يقدم حلاً لهذه المشكلة بوضع مخدم VPN و غالباً ما يكون هذا خاص لـ المخدم برمجياً.

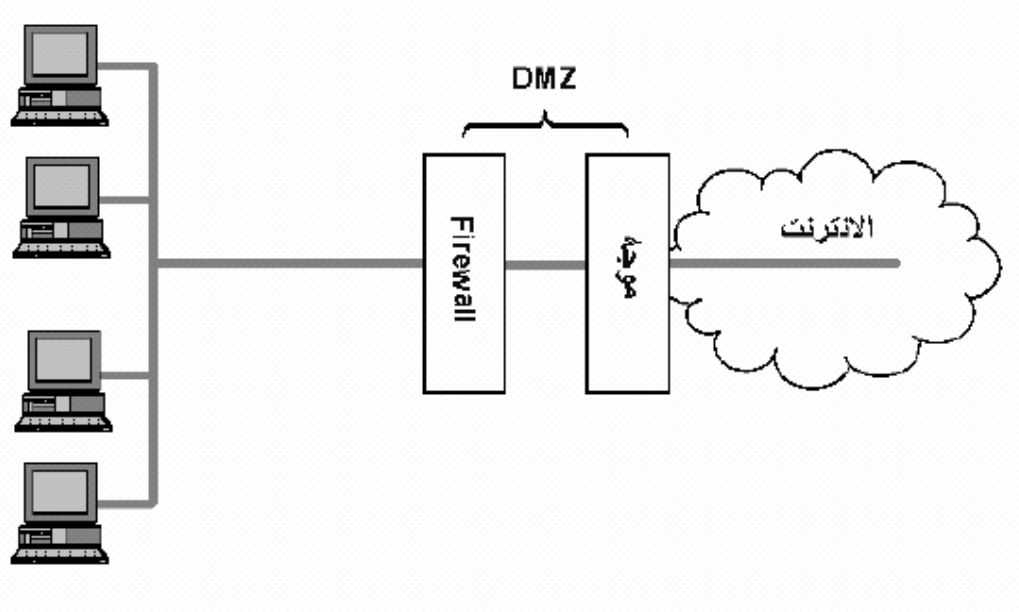
و VPN.فيما يلي توضيح لبعض البنى المقترحة من حيث VPN بالنسبة لـ DMZ الخيارات المختلفة لنقاط انتهاء



الشكل 7-6 مخدم VPN خلف الجدار النارى



الشكل 7-7 مخدم VPN على فرع من الشبكة



الشكل 7-8 جميع محطات العمل مزودة بـ VPN

الفصل السابع

الجزء العملي

1- إنشاء نفق IPsec لنظام لينوكس:

إن إنشاء نفق يقسم إلى جزأين الأول هو موديل النواة و يدعى Kernel module called ipsec_tunnel.o

و الثاني لإدارة ارتباطات السرية و النفق و يدعى Ipsecadm

بداية يجب تحميل الـ kernel إلى نواة نظام التشغيل لينوكس بتشغيل:

modprobe ipsec_tunnel.

الآن لدينا جهاز شبكة جديد يدعى ipsec0 و الذي نستطيع رؤيته بتشغيل ifconfig –a.

للأداة ipsecadm نمطين:

-الأول لإضافة و إزالة ترابطات الأمن وهو(SAs).

-الثاني لإضافة و إزالة الأنفاق التي يتم بناءها.

سنشرح طريقة بناء نفق من خلال السيناريو التالي:

بفرض أننا نريد بناء نفق بين مخدمين A و B :

وذلك بفرض و جود البارامترات التالية.

Host	A	B
Public IP address	1.2.3.4	5.6.7.8
Private IP address	10.0.1.1	10.0.2.1
Private network	10.0.1.0/24	10.0.2.0/24

إن IPsec يستخدم ترابطات السرية (SA) Security Associations و الذي يشكل اسماً آخر لبارامترات السرية بين المخدمين (A B) و الذي يتم توليده بشكل فريد باستخدام عنواني IPs و رقماً مؤلفاً من 32 بت يدعى بار متر فهرس السرية: Security Parameter Index(SPI)

إن الـ SPI يسمح بأكثر من SA بين زوج من المخدمات .

عندما يتفق على SA كلا الجزأين يتفقان على نمط SA و الذي يشفر و يوثق هو و الخوارزمية أيضاً.

و ليكن لدينا SA التالي :

SPI: 0x1000
Destination IP: 5.6.7.8
Source IP: 1.2.3.4
Encryption algorithm: 3DES
Encryption key size: 192 bits
… :Encryption key
Authentication algorithm: SHA-1
Authentication key size: 160 bits
… :Authentication key
Authentication HMAC size: 96 bits (default)

قبل أن نقوم بإنشاء SA نحن بحاجة إلى مفتاح و الذي من الممكن إنشاءه بسهولة باستخدام الأمر

ipsecadm key create command

لإنشاء مفتاح تشفير لخوارزمية 3DES في الملف:

the file /etc/ipsec/demo.ciph.key

قم بتشغيل:

ipsecadm key create 3des --file=/etc/ipsec/demo.ciph.key

-مفتاح التوثيق المؤلف من من عشرين بايت(120بت) يمكن توليده في الملف : etc/ipsec/demo.auth.key

بتشغيل الأمر :

ipsecadm key create sha1 --file=/etc/ipsec/demo.auth.key

أصبح بإمكاننا الآن استخدام الأداة ipsecadm لإنشاء الـ SA المذكورة سابقاً.

-cipher option :يحدد خوارزمية التشفير التي ستستخدم للتشفير.

-digest option:يحدد الخوارزمية المستخدمة للتوثيق.

-cipher name:يحدد بـ اسم cryptoapi الخاص به حيث أن الاسم الخاص بخوارزمية التشفير IPsec 3DES يعتمد على إصدار CryptoAPI الذي تقوم بتنصيبه.

-إذا كان لديك الإصدار الأخير فإن هذا الاسم هو 3des-cbc و لكن إذا كان لديك إصدار قديم فإن هذا الاسم هو des_ede3-cbc.

بإمكانك إيجاد الاسم حيث قمت بتنصيب ciphers and digest بالبحث ضمن المجلدات :

/proc/crypto/ cipher/ AND /proc/crypto/ digest

```
ipsecadm sa add
--spi=0x1000
--dst=5.6.7.8
--src=1.2.3.4 \
--cipher=3des-cbc \
--cipher-keyfile=/etc/ipsec/demo.ciph.key \
--digest=sha1 \
--digest-keyfile=/etc/ipsec/demo.auth.key \
 --duplex
```

بإمكاننا ملاحظة أن التوثيق اختياري لكن استخدام التشفير بدون توثيق ربما يعرضنا عند النقل إلى عدة أشكال من الهجمات الفعالة التي من الممكن أن تقوض الامن.

لماذا نستخدم زوج من البارامترات :إن إنشاء النفق يحتاج إلى اثنين SAs عند كل طرف "كل مخدم" و طالما انه من الشائع استخدام نفس إعدادات الأمن عند كل جهة بإمكاننا إنشاء زوج من SAs بإنشاء واحد يستخدم الـ duplex--

و لرؤية الـ SAs الاثنين بعد إنشائهم قم بتشغيل:

```
ipsecadm sa show
```

نلاحظ أن SAs يستخدم لكل حمولات IPsec ليس فقط من أجل الأنفاق,و لكن الآن لم نقم إلا بإنشاء النفق.

-الخطـوة التاليــة فــي إنشــاء النفـق تتمثـل فــي الأوامـر المطلـوب تنفيـذها بالنسـبة للمخدمين A و B :

للمخدم A: -- ipsecadm tunnel add ipsec1 --local=1.2.3.4 --remote=5.6.7.8

للمخدم B:-- ipsecadm tunnel add ipsec2 --local=10.0.0.11 --remote=10.0.2.1

ليس هناك حاجة لتحديد SPI و بإمكاننا تحديده إذا أردنا استخدام خيار spi– وإذا لم نرد استخدامه فإن العنوانين المحلي و البعيد يستخدمان لإيجاد SA مناسب.

-أما الآن فنحن بحاجة وضع رقم IP من أجل النفق الجديد الذي تم إنشاءه مؤخراً,و لكن كيف سيكون ذلك ؟

عندما تنشأ رزمة في جهاز ما عنوان الهدف يستخدم من قبل جدول التوجيه لإيجاد جهاز الخروج للاتصال و عنوان المصدر يوضع فيه عنوان ذلك الجهاز.

إذا أردنا إنشاء اتصال من المخدم A إلى جهاز في الشبكة الخاصة بالمخدم B فإن عنوان المصدر الموجود في الرزمة سيكون العنوان الخاص للمخدم A و الذي هو 10.0.1.1:

ifconfig ipsec1 10.0.1.1 up

الخطوة الأخيرة هي إنشاء قيمة مدخلة في جدول التوجيه و التي ستجعل الرزم المتوجهة للشبكة الخاصة عند المخدم B تتجه عبر الجهاز ipsec1 .

route add -net 10.0.2.0/24 dev ipsec1

بقي أن نقوم بنفس الفعل المكافئ على المخدم B.حيث لا حاجة لتوليد مفتاح جديد على المخدم B و إنما بإمكانك نسخ المفتاح الذي تم إنشاءه على المخدم A و ذلك بطريقة سرية و آمنة.

2- إعداد ويندوس CLIENT و

ويندوس SERVER

2-1 التجهيز

حتى تكون مستعد لعمل الشبكة يلزم التأكد من عدد من الامور منها

- خادم الـ VPN يكون موصول بشبكة الانترنت بخط DSL مع عنوان IP ثابت
- خادم الـ VPN يكون مثبت عليه أو على خادم ثاني في نفس الشبكة خدمة DHCP
- عملاء الوصول البعيد لهم حساب في الشبكة بإسم وكلمة مرور
- اجهزة العملاء قادرة على تأسيس الإتصال بتدريب اصحابها أو تقوم بتجهيزها أنت .

2-2تجهيز خادمVPN

لتجهيز الخادم لقبول إتصالات VPN نحتاج إلى تثبيت الخدمة RRAS وهي تكون مثبته مع تثبيت الويندوز 2000 ولكن تكون غير ممكنه وتحتاج إلى تفعيل ،، وسنقوم بتمكين الخدمة على ملقم ويندوز 2000 ،، ولكن نفترض في هذا الشرح وجود خدمة الـ DHCP على نفس الخادم ،، مع وصول دائم بالانترنت مع معرفتك بعنوان IP الثابت ،، سنقوم في مثالنا هذا بإعداد مخدم VPN PPTP ، لأن هذا المخدم يتعبر اسهل في الاعداد والوصول إليه بسبب استخدامه لوثائق Logon للمستثمر فقط ، اما مخدم VPN L2TP فهويستخدم في كثير من الحالات بين الخوادم لما له من مزايا في الأمن اكبر.

1. اختر Programs > Administrative Tools > Routing and Remote Accessثم من على اسم الخادم بالزر الايمن اختر Configure And Enable Routing And Remote Access
2. يفتح لك معالج التثبيت انقر Next
3. من هذه النافذة اختر الخيار شبكة VPN كما في الصورة

4. في النافذة التالية تأكد من وجود البروتوكول TCP/IP واترك الخيار المختار كما هو ثمNext
5. تشاهد اتصالات الخادم ومنها إتصال الانترنت اختر الاتصال الدائم ثم Next
6. في هذه النافذة تختار أما اسناد عناوين محددة للعملاء أو اسناد العناوين من DHCPإقبل الخيار Automatically لقبول استخدام DHCP المحلي للعملاء المتصلين
7. من أخر نافذة اختر الخيار التلقائي فيها وهي عدم استخدام الخدمة RADIUSلتحقق من صحة المعلومات المقدمة من المتصلين ، لان توثيق الويندوز التلقائي يفي بكل متطلباتك الأمنية عندما تكون تملك خادم RASوحيد على الشبكة انقرNext
8. تظهر لك رسالة تحذير من DHCP وهي غير ضرورية إلا في حالة وجود مخدم DHCP على شبكة فرعية آخرى انقر OK
9. تظهر لك نافذة التجهيز 

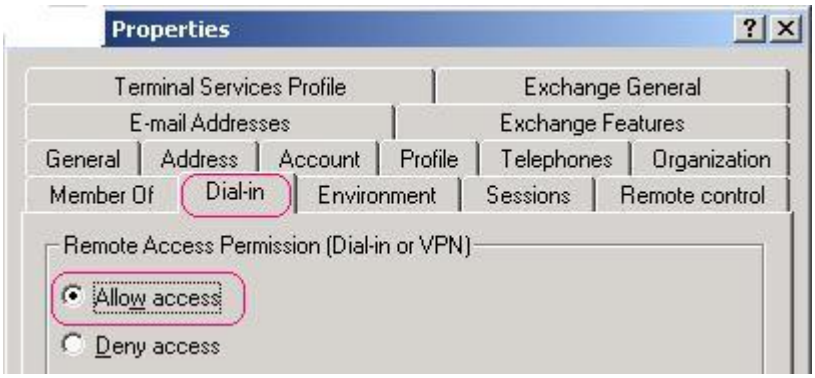
لعمل الخدمة

الآن تشاهد العلامة الحمراء التي كانت على اسم الخادم اصبحت بلون اخضر ، وبهذا تكون قد مكنت الملقم من الاستعداد لإستقبال العملاء عبر بوابة الانترنت ،

وطبعاً مع هذا التثبيت الافتراضي توجد بعض الخصائص التي من الممكن تغيرها حسب حاجتك مثل عدد المنافذ لكل بروتوكول ولكل بروتوكول عند التثبيت عدد 128 منفذ يمكن تخفيض منافذ البروتوكول PPTP إلى 1 منفذ ولكن هذا عدد قليل جداً حدد عدد معقول ، والبروتوكول L2TP يمكن ان تحدد الرقم 0 يعني لا يوجد منفذ ، لتحديد أو إلغاء المنافذ من علامة + بجانب اسم خادم VPN تظهر لك Portsبالماواس بالزر الايمن ثم اختر خصائص ثم من النافذة اختر احد البروتوكولين ثم من الزر Configure ثم امام Maximum ports اكتب الرقم المراد

3-2 تجهيز العميل

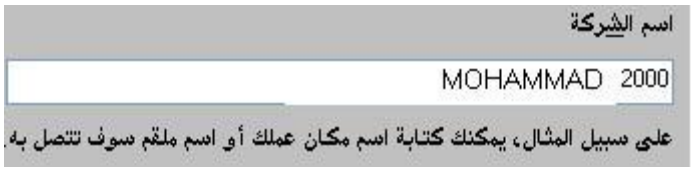
سنقوم بتجهيز جهاز ويندوز xp-p لإستخدام الانترنت وسيط للوصول إلى خادم VPN، ولكن قبل تجهيز العميل يجب أن تتأكد من خصائص العميل على خادم VPNهل يملك حق الدخول عبر الاتصال الهاتفي ام لا ، ولتتأكد من ذالك ادخل على خصائص المستخدم ثم اختر كما في الصورة



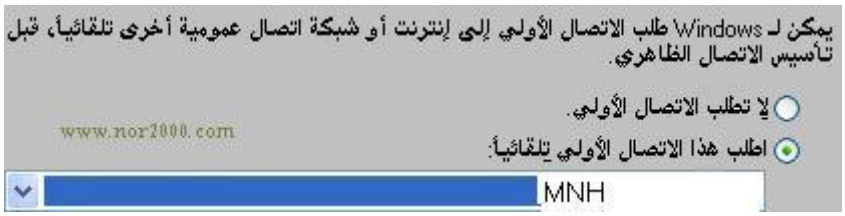
الآن من الويندوز XP سنقوم ببعض الخطوات البسيطة لتكوين الاتصال من اتصال شبكة الاتصال اختر إنشاء اتصال جديد شاشة الترحيب اضغط على التالي من هذه الشاشة اختر

ثم من النافذة التالية اختر

ثم اكتب اسماً لهذا الاتصال وليكنMOHAMMAD2000



ثم من هنا اختر الاتصال الاولي الذي ترغب ان تستخدمه في الوصول للانترنت قبل الوصول إلى ملقم VPN وكما في المثال اخترنا الاتصالة MNH



وطبعاً هذا الاتصال يكون معد مسبقاً ، وإذا كان غير موجود من قبل إتصال بالانترنت أنشاء اولاً إتصال بأنترنت مع موفر خدمةasp

الآن اهم خطوة وهي كتابة اسم المضيف أو عنوان IP صحيح لملقمVPN

اكتمل بناء الاتصال اختر من النافذة الاخيرة إنهاء

ستجد في اتصالات شبكة الاتصال ايكون جديد بإسم mohammad2000 للإتصال بالشبكة الخصوصية الوهمية

تعديل خصائص الاتصال

بعض الخصائص تحتاج إلى تعديل حسب وضع ملقم VPN لديك وفي مثالنا هذا نحتاج الى التعديل التالي

افتح خصائص هذا الاتصال بالزر الايمن على اسمه ثم من علامة التبويب الأمان علم على الخيار استخدام اسم تسجيل الدخول إلى Windows وكلمة المرور

ثم من علامة التبويب شبكة الاتصال من القائمة المنسدلة اختر الخيار PPTP VPN، ولو تركته كما كان سابقاً سيفشل الوصول إلى الملقم في اكثر الاحيان

4-2 إجراء الإتصال بمخدمVPN

1. من قائمة الاتصالات اختر الاتصال بمقدم خدمة الانترنت لديك وفي مثالنا هذا الاتصال جهينة

2. وبعد تسجيل الدخول على الانترنت انقر نقراً مزدوجاً على إتصال VPN وهو لدينا بإسم MOHAMMAD2000
3. سيحاول البحث عن مسار العنوان في الانترنت وإذا كان عنوان ملقم VPN الذي كتبته في خصائص الاتصال صحيحاً ستجد الملقم جاهز لإنشاء جلسة عمل معك
4. وستظهر لك نافذة تسألك عن اسم الدخول ID وكلمة المرور ، اكمل كل المعلومات ثمConnect
5. ستكون في هذا الحالة موصول مع الشبكة وكأنك في نفس المقطع الفيزيائي

المراجع

- مجلاد مشاري السبيعي: الشبكات الخاصه الوهميه النظريه والتطبيقيه .

- د.وجدي عبد الرحيم :" التشفير بالطرق الكلاسيكية" ،

- د.حسن داوود :" الحاسب و أمن المعلومات" ، الرياض ، مكتبة الملك فهد الوطنية

- المهندس ناهي يوسف الشاهين :" دراسة وتصميم خوارزمية تشفير للبيانات المنقولة عبرالشبكة" ، دراسة في جامعة دمشق ، باشراف الدكتور نديم شاهين

- Cisco (2000), Cisco IOS Software Feature: Network-Layer Encryption. White Paper "encrp_wp.pdf".
- The Laws of Cryptography with java code , by Neal R.Wanger
- Introduction to cryptography with Java applets, David Bishop
- History About Cryptography and Crypto Devices and Arabic Cryptographer (Alkindi, Taher Algamal)
- عن الانترنت :

- http://www.arablaw.org/Information%20Security.htm
- http://informationsecurity.techtarget.com
- http://www.boosla.com/books/privacy.pdfEncryption
- http://www.itep.ae/arabic/EducationalCenter/Articles
- http://www.techworld.com/security

الفهرس

الفصل الرابع :